Scaffolds in Non-classical Hopf-Galois Structures

Submitted by

Chinnawat Chetcharungkit

to the University of Exeter as a thesis for the degree of Doctor of Philosophy in Mathematics, July 2018.

I certify that all the material in this thesis which is not my own work has been identified and that no material is included for which a degree has previously been conferred upon me.

.....

Chinnawat Chetcharungkit

Abstract

For an extension of local fields, a scaffold is shown to be a powerful tool for dealing with the problem of the freeness of fractional ideals over their associated orders (Byott, Childs and Elder: *Scaffolds and Generalized Integral Galois Module Structure*, Ann. Inst. Fourier, 2018). The first class of field extensions admitting scaffolds is 'near one-dimensional elementary abelian extension', introduced by Elder (*Galois Scaffolding in One-dimensional Elementary Abelian Extensions*, Proc. Amer. Math. Soc. 2009). However, the scaffolds constructed in Elder's paper arise only from the classical Hopf-Galois structure. Therefore, the study in this thesis aims to investigate scaffolds in non-classical Hopf-Galois structures. Let L/K be a near one-dimensional elementary abelian extension of degree p^2 for a prime $p \geq 3$. We show that, among the $p^2 - 1$ non-classical Hopf-Galois structures on the extension, there are only $p - 1$ of them for which scaffolds may exist, and these exist only under certain restrictive arithmetic condition on the ramification break numbers for the extension. The existence of scaffolds is beneficial for determining the freeness status of fractional ideals of $\mathfrak{O}_L$ over their associated orders. In almost all other cases, there is no fractional ideal which is free over its associated order. As a result, scaffolds fail to exist.

Acknowledgements

With my attempt alone, this thesis would not have been possible. Over the past three years, I have received numerous supports and guidance from many people.

First and foremost, I would like to thank Prof Nigel Byott, my supervisor. With his exceptional idea, advice and patience, the completion of my PhD study could come true smoothly. Next, my deep gratitude goes to my family, Thai friends and PhD office-mates for their endless encouragement. Also, I would have felt guilty without mentioning Prof Vichian Laohakosol, Assoc Prof Nongnuch Sukvaree and her colleagues for invaluable foundations of mathematics. Besides this, I have reckoned that studying in non-native Thai-speaking countries like UK is very tough. Yet, I could get through this challenging time with English knowledge and skills from Chamaipak Tayjasanant, my beloved English instructor. Moreover, my sincere gratitude goes to the Development and Promotion of Science and Technology Talents Project (DPST) for an inordinate amount of the funding for my PhD study.

In terms of the research, I am really grateful to Prof Griff Elder who introduced a powerful weapon like Galois scaffold.

Last but not least, especially thanks to Surat Maneejansook for being an effective catalyst for writing up this thesis.

Contents

Chapter 1

Introduction

The so-called normal basis theorem, which states that for a finite Galois extension L/K with Galois group G there exists an $x \in L$ such that the set $\{g(x) : g \in G\}$ is a basis for L/K, is an origin of Galois module theory. There have been many problems, including our study, inspired by this theorem. For example, any element y in L can be written as $\sum_{g\in G} k_g g(x)$ for some $k_g \in K$. Equivalently, L is a free module of rank one over the group ring $K[G]$. From this idea, when L/K is an extension of global or local fields, it is natural to ask whether an analogous result holds at integral level. In other words, is $\mathfrak{O}_L$ a free module of rank one over $\mathfrak{O}_K[G]$? In the local setting, this question was answered by Noether's theorem. The necessary and sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{O}_K[G]$ is that L/K is tamely ramified. After that, many authors have tried to investigate this question for various classes of wildly ramified extensions. By Noether's theorem, in the wild case, $\mathfrak{O}_L$ is not a free module of rank one over $\mathfrak{O}_K[G]$. Later, it was found that the associated order $\mathfrak{A}_{K[G]} = \{\alpha \in K[G] : \alpha\mathfrak{O}_L \subseteq \mathfrak{O}_L\}$ was an eligible candidate over which $\mathfrak{O}_L$ could be free. Yet, how to address such a question is still very difficult unless we have a powerful weapon.

The concept of Galois scaffolds first appeared in Elder's paper [El09]. Let $K = k((T))$ be a local function field with perfect residue field k of charac-

teristic $p > 0$. For a totally ramified abelian extension L/K of degree p^{n+1} with a special assumption, Elder constructed $n+1$ elements from the group ring $K[G] := K[\mathrm{Gal}(L/K)]$, say $\{\Psi_i\}_{i=0}^{n}$ and chose an appropriate integer (called the integer certificate) such that if $\rho \in L$ and $v_L(\rho)$ is equal to the integer certificate, then the set $\{v_L(\Psi_0^{a_0}\Psi_1^{a_1}\cdots\Psi_n^{a_n}\rho) : 0 \leq a_i \leq p-1\}$ forms a complete set of residues modulo p^{n+1}, where v_L is the nomalised valuation on L. If a field extension possesses the two ingredients which satisfy the property, we say it admits a Galois scaffold. In particular, this gives us a basis for L/K.

Nevertheless, the question of the existence of a class of field extensions satisfying the special assumption cannot be ignored. Consequently, in the last section of [El09], near one-dimensional elementary abelian extensions are created. Undoubtedly, due to the construction, they satisfy such an assumption and hence admit Galois scaffolds. Moreover, one of the benefits of Galois scaffolds can be seen in [BE14]. Going back to the Galois module theoretic view, it enables us to determine a necessary and sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{K[G]}$, the associated order of $\mathfrak{O}_L$, in the group ring $K[G]$.

Later, the notion of Galois scaffolds is generalised in [BCE] in the sense that the suitable $n+1$ elements can be picked not only from the group ring $K[G]$ but also from any K-algebra of dimension p^{n+1} acting faithfully on L. As a result, the phrase 'Galois scaffold' becomes just 'scaffold'. Also, the generalisation of associated orders in any K-algebra, as well as the investigation of the freeness of fractional ideals of $\mathfrak{O}_L$ over their generalised associated orders, are provided in this paper. However, in this thesis, the study is restricted to certain type of K-Hopf algebras giving Hopf-Galois structures rather than general K-algebras. We also say that a Hopf-Galois structure is classical if the Hopf algebra acting on the field is $K[G]$; otherwise, it is called non-classical.

Therefore, it can be said that scaffolds exist in the classical Hopf-Galois struc-

ture on the class of near one-dimensional elementary abelian extensions, but the question of the existence of scaffolds in non-classical Hopf-Galois structures is still open. The main purpose of this study is to investigate such a problem in near one-dimensional elementary abelian extensions of degree p^2 with $p \geq 3$. Furthermore, if they exist, in the light of the main result in [BCE], we obtain a necessary and sufficient condition for a fractional ideal of $\mathfrak{O}_L$ to be free over its associated order in a given Hopf algebra.

For an elementary abelian extension of degree p^2 (and thus near one-dimensional elementary abelian extensions are included), it is known that each of the $p+1$ subgroups of order p in Galois group generates $p-1$ non-classical Hopf-Galois structures. This yields precisely p^2-1 non-classical Hopf-Galois structures on the extension.

In this research, it is found that scaffolds can exist only in $p-1$ of the non-classical Hopf-Galois structures on any near one-dimensional elementary abelian extension of degree p^2, and then only under certain arithmetic conditions. Therefore, in these structures, we can answer the freeness question of fractional ideals. In terms of the other structures, which are the majority of the Hopf-Galois structures on the extension, we can show that scaffolds fail to exist, and indeed no fractional ideal is free over its associated order. Unfortunately, the study cannot cover a few marginal cases under some arithmetic conditions in the minority of the Hopf-Galois structures.

This thesis contains eight chapters. All the background material needed in order to conduct this research is given in Chapter 2. This includes basic definitions and the essential results from the papers cited above.

Since there are plenty of Hopf-Galois structures on near one-dimensional elementary abelian extensions of degree p^2, we introduce the 'unified language' in

Chapter 3. It enables us to work with all the non-classical Hopf-Galois structures simultaneously. The descriptions of all the Hopf algebras on the extensions, as well as nice generators for them, are also presented in this chapter.

The aim of Chapter 4 is to understand the actions of Hopf algebras, obtained from Chapter 3, on near one-dimensional elementary abelian extensions. As a formula for the actions is intractable, an ordering on terms in L is introduced. This ordering acts like a compass navigating us to pay attention to certain significant terms, which become main keys in the next chapter.

Chapter 5 contains the main lemma playing a major role in the proof of the non-freeness of fractional ideals in Hopf-Galois structures on near one-dimensional elementary abelian extensions. The proof can be seen in Chapter 6. Sadly, there is a type of Hopf-Galois structures to which the main lemma cannot be applied. In one case of this type, which is clearly stated in the last section of Chapter 6, the study cannot get through; whereas in the other case, we can construct scaffolds, the most desirable object in this thesis. This can be seen in Chapter 7. Lastly, the final chapter is responsible for providing the consequences of the results in Chapter 6 and 7. Also, the final theorem summarising all the main results obtained in this thesis is presented in this final chapter.

Notations

For the reader's convenience, the following notations used throughout this report are given here. We set p to be a prime number at least 3. We denote by C_p and $\mathbb{F}_p$ the cyclic group with p elements and the finite field of order p respectively. As far as local fields are concerned, we use subscripts to denote the field of reference. For example, let L/K be a finite Galois extension of local fields. Then, π_K is a prime element of K, π_L is a prime element of L. Let v_K (resp. v_L) be the valuation

on K (resp. L) normalised so that $v_K(\pi_K) = 1$ (resp. $v_L(\pi_L) = 1$). We define $\mathfrak{O}_L = \{x \in L : v_L(x) \geq 0\}$ to be the valuation ring of L and $\mathfrak{P}_L = \pi_L \mathfrak{O}_L$ to be the maximal ideal of $\mathfrak{O}_L$. Also, we denote by G_i the ith ramification group of G i.e. $G_i = \{\sigma \in G : v_L((\sigma - 1)x) \geq i + 1 \ \forall x \in \mathfrak{O}_L\}$.

Chapter 2

Background

This chapter is dedicated to collecting all materials required for doing this research. Since we investigate Hopf-Galois structures on certain extensions of local fields, we begin with introducing Hopf algebras, followed by Hopf-Galois structures. Then, some background on local fields is provided. Lastly, the concept of Galois scaffolds, along with its generalisation and application, are presented.

2.1 Hopf Algebras

Before defining a Hopf algebra, we need to define an algebra and a bialgebra.

Definition 2.1.1. Let R be a commutative ring with unity and let A be an R-module. A triple (A, μ, ι), where $\mu : A \otimes_R A \to A$ and $\iota : R \to A$, is said to be an *R-algebra* if the following diagrams commute:

• Associativity:

$$\begin{array}{ccc} A \otimes_R A \otimes_R A & \xrightarrow{\mu \otimes 1} & A \otimes_R A \\ \downarrow{\scriptstyle 1 \otimes \mu} & & \downarrow{\scriptstyle \mu} \\ A \otimes_R A & \xrightarrow[\mu]{} & A \end{array}$$

• Unitarity:

$$\begin{array}{ccc} A \otimes_R R & \xrightarrow{1\otimes\iota} & A \otimes_R A \\ \| & & \downarrow{\scriptstyle \mu} \\ A \otimes_R R & \xrightarrow[module\ mult.]{} & A \end{array}$$

and

$$\begin{array}{ccc} R \otimes_R A & \xrightarrow{\iota\otimes 1} & A \otimes_R A \\ \| & & \downarrow{\scriptstyle \mu} \\ R \otimes_R A & \xrightarrow[module\ mult.]{} & A \end{array}$$

We call μ the multiplication map and ι the unit map.

For instance, we see that R is an R-algebra.

Definition 2.1.2. Let R be a commutative ring with unity and let A be an R-algebra. A triple (A, Δ, ϵ), where $\Delta : A \to A \otimes_R A$ and $\epsilon : A \to R$ are R-algebra homomorphisms, is said to be an *R-bialgebra* if the following diagrams commute:

• Coassociativity:

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_R A \\ {\scriptstyle \Delta}\downarrow & & \downarrow{\scriptstyle \Delta\otimes 1} \\ A \otimes_R A & \xrightarrow[1\otimes\Delta]{} & A \otimes_R A \otimes_R A \end{array}$$

• Counitarity:

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_R A \\ \| & & \downarrow{\scriptstyle 1\otimes\epsilon} \\ A & \xleftarrow{module\ mult.} & A \otimes_R R \end{array}$$

and

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_R A \\ \| & & \downarrow{\scriptstyle \epsilon\otimes 1} \\ A & \xleftarrow{module\ mult.} & R \otimes_R A \end{array}$$

We call Δ the comultiplication map and ϵ the counit map.

For the sake of computation, it is a wise idea to use the notation of Sweedler to write $\Delta(a) = \sum_{(a)} a_{(1)} \otimes a_{(2)} \in A \otimes_R A$ for all $a \in A$. For instance, we have

$$\begin{aligned} (1 \otimes \Delta)\Delta(a) &= (1 \otimes \Delta)\left(\sum_{(a)} a_{(1)} \otimes a_{(2)}\right) \\ &= \sum_{(a)} a_{(1)} \otimes \Delta(a_{(2)}) \\ &= \sum_{(a,a_{(2)})} a_{(1)} \otimes a_{(2)_{(1)}} \otimes a_{(2)_{(2)}} \end{aligned}$$

and $(\Delta \otimes 1)\Delta(a) = \sum_{(a,a_{(1)})} a_{(1)_{(1)}} \otimes a_{(1)_{(2)}} \otimes a_{(2)}$. However, by the coassociativity, we have $\sum_{(a,a_{(2)})} a_{(1)} \otimes a_{(2)_{(1)}} \otimes a_{(2)_{(2)}} = \sum_{(a,a_{(1)})} a_{(1)_{(1)}} \otimes a_{(1)_{(2)}} \otimes a_{(2)}$ and usually write $\sum_{(a)} a_{(1)} \otimes a_{(2)} \otimes a_{(3)}$ instead.

Now, we are ready to define a Hopf algebra.

Definition 2.1.3. Let R be a commutative ring with unity and let H be an R-bialgebra equipped with the multiplication map μ, the unit map ι, the comultiplication map Δ and the counit map ϵ. Then, H is called an *R-Hopf algebra* if there is an R-module homomorphism $\lambda : H \to H$ called the *antipode map* such that

(i) λ is an R-algebra antihomomorphism i.e. $\lambda(h_1h_2) = \lambda(h_2)\lambda(h_1)$ for all $h_1, h_2 \in H$;

(ii) λ is an R-coalgebra antihomomorphism i.e. $\Delta\lambda(h) = (\lambda \otimes \lambda)\tau\Delta(h)$ where $\tau : H \otimes_R H \to H \otimes_R H$ is the *switch map* defined as $\tau(h_1 \otimes h_2) = h_2 \otimes h_1$ for all $h_1, h_2 \in H$;

(iii) λ satisfies $\mu(1 \otimes \lambda)\Delta = \iota\epsilon = \mu(\lambda \otimes 1)\Delta$.

Example 2.1.4. Let G be a finite group and K a field. Then, the group ring

$$K[G] = \left\{ \sum_{g \in G} k_g g : k_g \in K \right\}$$

is a K-Hopf algebra with $\Delta(g) = g \otimes g$, $\epsilon(g) = 1$ and $\lambda(g) = g^{-1}$.

2.2 Hopf-Galois Structures

Let L/K be a finite Galois extension with Galois group G. According to the example above, $K[G]$ is a K-Hopf algebra and one can make it act on L intuitively i.e. $\sum_{g \in G} k_g g \cdot x = \sum_{g \in G} k_g g(x)$ for any $x \in L$. In particular, we have

$$\sum_{g \in G} k_g g \cdot xy = \sum_{g \in G} k_g g(x)g(y) = \sum_{g \in G} k_g (g \cdot x)(g \cdot y)$$

for any $x, y \in L$. With the intention of generalising this idea to any Hopf algebra acting on an algebra, we define a module algebra.

Definition 2.2.1. Let R be a commutative ring with unity. Let H be an R-Hopf algebra and S an R-algebra. Then S is called an *H-module algebra* if

(i) S is an H-module;

(ii) We have $h(s_1 s_2) = \sum_{(h)} (h_{(1)} s_1)(h_{(2)} s_2)$ and $h1_S = \epsilon(h)1_S$ for all $h \in H$ and $s_1, s_2 \in S$.

Definition 2.2.2. Let R be a commutative ring with unity. Let H be an R-Hopf algebra, and let S be a finite commutative R-algebra such that S is an H-module algebra. Then S is said to be an *H-Galois extension of R*, or *H-Galois over R* for short, if the R-module homomorphism

$$j : S \otimes_R H \to End_R(S)$$

defined as $j(s \otimes h)(t) = s(ht)$ for $s, t \in S, h \in H$ is an R-module isomorphism.

If S is an H-Galois extension of R, we sometimes say that *H gives a Hopf-Galois structure on the extension*. Although, in the definition above, S and R can be commutative rings, we consider only the special case where S is a finite Galois extension of a field R.

The question of how many Hopf-Galois structures there are on a finite Galois extension is very intriguing. In order to deal with this question, we need a powerful tool which is the theorem of Greither and Pareigis. Moreover, the theorem can even tell us what all Hopf algebras giving Hopf-Galois structures on the extension look like and how the Hopf algebras act on the given field. Before stating this theorem, we have to mention certain unavoidable concepts.

Throughout the rest of this section, all materials are selected from [Ch00], [By96] and [By02], with some minor modifications to be in accordance with our situation. In spite of the fact that the theorem of Greither and Pareigis requires a field extension to be finite and separable, we only consider finite Galois extensions in this study.

Definition 2.2.3. Denote by $\mathrm{Perm}(X)$ the group of permutations of the finite set X. Let N be a subgroup of $\mathrm{Perm}(X)$. Then, we say N is *regular* provided that it satisfies any two of the following conditions:

(i) The cardinalities of N and X are equal;

(ii) N acts transitively on X;

(iii) For each $x \in X$, its stabiliser $\mathrm{Stab}_N(x) = \{\eta \in N : \eta(x) = x\}$ is trivial.

It can be verified that if two of the conditions above are satisfied, then the other will hold automatically.

Let L/K be a finite Galois extension with Galois group G. In our setting, the set X is nothing but G.

Definition 2.2.4. (i) The *left translation map* $\lambda : G \to \mathrm{Perm}(G)$ is defined by

$$\lambda(g_1)(g_2) = g_1 g_2 \quad \text{for all } g_1, g_2 \in G.$$

(ii) The *right translation map* $\rho : G \to \mathrm{Perm}(G)$ is defined by

$$\rho(g_1)(g_2) = g_2 g_1^{-1} \quad \text{for all } g_1, g_2 \in G.$$

These maps are highly crucial. Not every Hopf algebra can give us a Hopf-Galois structure on a given extension but only those filtered by λ in some sense. In terms of the latter, the map ρ is responsible for giving us the classical Hopf-Galois structure.

Definition 2.2.5. We say that a regular subgroup N of $\mathrm{Perm}(G)$ is *normalised by* $\lambda(G)$ if $N = \lambda(g)N\lambda(g^{-1})$ for all $g \in G$.

Proposition 2.2.6. *If N is normalised by $\lambda(G)$, then an action of G on $L[N]$ can be given by*

$$g \cdot \sum_{\tau \in N} x_\tau \tau = \sum_{\tau \in N} g(x_\tau)\lambda(g)\tau\lambda(g^{-1})$$

for $g \in G$ and $\sum_{\tau \in N} x_\tau \tau \in L[N]$.

Proof. This is part of the proof of [Ch00, 6.7]. □

Theorem 2.2.7 (**Greither and Pareigis**). *Let L/K be a finite Galois extension with group G. Then, there is a bijection between regular subgroups N of $Perm(G)$ normalised by $\lambda(G)$ and Hopf-Galois structures on L/K. In particular, a regular subgroup N corresponds to a Hopf algebra $L[N]^G := \{x \in L[N] : g \cdot x = x \ \forall g \in G\}$.*

Proof. See [Ch00, 6.8] □

The Greither-Pareigis theorem is one of the vital tools since it gives us all Hopf algebras giving Hopf-Galois structures on an extension. The next question is how those Hopf algebras act on the field L. One can tackle this question by consulting [By02, (2.2)].

The algebra $L[N]$ acts on $\mathrm{Map}(G, L)$, the algebra of functions $f : G \to L$, by

$$((xn) \cdot f)(g) = xf\left(n^{-1}(g)\right)$$

for $x \in L$, $n \in N$, $g \in G$. One can identify $\mathrm{Map}_G(G, L)$, the subalgebra of $\mathrm{Map}(G, L)$ of G-equivalent functions $G \to L$ (where G acts on itself by left translations), with L via $f \mapsto f(1_G)$.

Let $l \in L$. Then, there exists $f \in \mathrm{Map}_G(G, L)$ such that $l = f(1_G)$ and hence $f(g) = g(l)$ for all $g \in G$. Let $\sum_{\tau \in N} x_\tau \tau \in L[N]^G$. Since $\sum_{\tau \in N} x_\tau \tau \in L[N]$ and $f \in \mathrm{Map}(G, L)$, the action of $L[N]$ on $\mathrm{Map}(G, L)$ gives $\overline{f} : G \to L$ defined by

$$\overline{f}(g) = \sum_{\tau \in N} x_\tau f\left(\tau^{-1}(g)\right).$$

To see how $\sum_{\tau \in N} x_\tau \tau$ acts on l, we first need to check that $\overline{f}$ is in $\mathrm{Map}_G(G, L)$.

Let $h \in G$. We compute

$$\begin{aligned}
h\left(\overline{f}(g)\right) &= h\left(\sum_{\tau\in N} x_\tau f\left(\tau^{-1}(g)\right)\right) \\
&= h\left(\sum_{\tau\in N} x_\tau f\left(\tau^{-1}(h^{-1}hg)\right)\right) \\
&= h\left(\sum_{\tau\in N} x_\tau f\left(\tau^{-1}\lambda(h^{-1})(hg)\right)\right) \\
&= h\left(\sum_{\tau\in N} x_\tau f\left(h^{-1}h\left(\tau^{-1}\lambda(h^{-1})(hg)\right)\right)\right) \\
&= \sum_{\tau\in N} h(x_\tau) f\left(h\left(\tau^{-1}\lambda(h^{-1})(hg)\right)\right) \\
&= \sum_{\tau\in N} h(x_\tau) f\left(\left(\lambda(h)\tau\lambda(h^{-1})\right)^{-1}(hg)\right) \\
&= \sum_{\tau\in N} x_\tau f\left(\tau^{-1}(hg)\right) \qquad\qquad (\because \sum_{\tau\in N} x_\tau\tau \in L[N]^G) \\
&= \overline{f}(hg).
\end{aligned}$$

Hence, $\overline{f} \in \mathrm{Map}_G(G, L)$. Then, we have

$$\sum_{\tau\in N} x_\tau\tau \cdot l = \sum_{\tau\in N} \left((x_\tau\tau)\cdot f\right)(1_G) = \sum_{\tau\in N} x_\tau f\left(\tau^{-1}(1_G)\right) = \sum_{\tau\in N} x_\tau\tau^{-1}(1_G)(l). \tag{2.2.1}$$

Note that (2.2.1) tells us how $L[N]^G$ (not $L[N]$) acts on L.

2.3 Local Fields

To define local fields, we first introduce the concept of discrete valuations on fields.

Definition 2.3.1. Let K be a field. The surjective group homomorphism

$$v : K \setminus \{0\} \to \mathbb{Z}$$

is called a *discrete valuation* on K if for every $x, y \in K \setminus \{0\}$ with $x \neq -y$, we have $v(x+y) \geq \min\{v(x), v(y)\}$. We also make the convention that $v(0) = \infty$.

When a field K equipped with a valuation v_K, we define the ring of integers of its as

$$\mathfrak{O}_K := \{x \in K : v_K(x) \geq 0\}.$$

Then, one can show that $\mathfrak{O}_K$ is a local PID with the unique maximal ideal

$$\mathfrak{P}_K := \{x \in K : v_K(x) > 0\}.$$

An element generating $\mathfrak{P}_K$ is called a uniformiser, say π_K. Note that $v_K(\pi_K) = 1$. We call the quotient $\mathfrak{O}_K/\mathfrak{P}_K$ the residue field of (K, v_K).

Each valuation on K induces a metric defined as

$$d_{v_K,c}(x, y) = c^{v_K(x-y)}$$

when $0 < c < 1$. In fact, for $0 < c_1, c_2 < 0$, the metrics d_{v_K,c_1} and d_{v_K,c_2} generate the same topology (see e.g. [Ef06, Chapter 9] for the proof). Therefore, we can omit the constant c and write just d_{v_K}.

Definition 2.3.2. The valuation v_K on K is said to be *complete* if the metric space (K, d_v) is complete.

Now, we can define a local field.

Definition 2.3.3. A *local field* is a complete discrete valuation field with perfect residue field.

Let K be a local field and L/K a finite extension. Then, L is a local field with the valuation v_L prolonging v_K with index $e(L/K)$. The index $e(L/K)$ is known as the *ramification index*, which is the number such that $\pi_K \mathfrak{O}_L = \pi_L^{e(L/K)} \mathfrak{O}_L$. See e.g. [Se79, Chapter II, §2, Corollary 2]). In particular, if the extension is Galois, we define:

Definition 2.3.4. Let L/K be a finite Galois extension with Galois group G. The *ramification group* G_i ($i \in \mathbb{Z}$ and $i \geq -1$) of G is the subgroup

$$G_i := \{\sigma \in G : v_L(\sigma(x) - x) \geq i + 1 \ \forall x \in \mathfrak{O}_L\}.$$

Hence, we have a filtration of normal subgroups of G [Se79]:

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq \langle e \rangle.$$

It is possible that some consecutive ramification groups are equal. Considering the subscript j such that $G_j \supsetneq G_{j+1}$ becomes interesting. We say that j is a *ramification break number* for L/K if $G_j \supsetneq G_{j+1}$.

Through the notion of ramification groups, we can classify extensions of local fields.

Definition 2.3.5. Let K be a local field. Then a finite Galois extension L/K is said to be:

- *unramified* if $G_0 = 1$;
- *ramified* if $G_0 \neq 1$;
- *totally ramified* if $G_0 = G$;
- *tamely ramified* if $G_1 = 1$; and
- *wildly ramified* if $G_1 \neq 1$

2.4 Scaffolds and Integral Hopf-Galois Module Structure

We first present the concept of Galois scaffolds, especially the exposition of the special assumption mentioned in Chapter 1 and a class of field extensions admitting

Galois scaffolds. However, there is no explicit definition of Galois scaffold in [El09]. Thus, the well-organised definition of Galois scaffold in a generalised version, called scaffold, is presented in Section 2.4.2.

The concept of Galois scaffolds is first used as a tool in [BE14] to investigate a classic question in Galois module structures i.e. the freeness of the valuation ring over its associated order. Moreover, the generalisation of these ideas is published in [BCE]. Namely, the concept of scaffolds is employed to investigate such a classic question but in a generalised version, which is finding a condition for fractional ideals to be free over their associated orders in a Hopf algebra.

2.4.1 Galois Scaffolds

Let $K = k((T))$ be a local function field with perfect residue field k of characteristic $p > 0$. Let K_n/K be a totally ramified abelian extension of degree p^{n+1} with the Galois group G. Assume that the ramification break numbers for this extension are $b_1 < b_2 < ... < b_m$. Hence, we have

$$G = G_{b_1} \supsetneq ... \supsetneq G_{b_m} \supsetneq G_{b_{m+1}} = \langle e \rangle.$$

Next, using the fact that every quotient of consecutive ramification groups G_i/G_{i+1} is elementary abelian (see [Se79, Chapter IV, §2, Corollary 3]), we can extend the series to $n+2$ subgroups

$$G = G_{(0)} \supsetneq G_{(1)} \supsetneq ... \supsetneq G_{(n)} \supsetneq G_{(n+1)} = \langle e \rangle$$

such that $G_{(i)}/G_{(i+1)} \cong C_p$ and for each $j \in \{1, 2, ..., m+1\}$ there exists $i \in \{0, 1, ..., n+1\}$ such that $G_{(i)} = G_{b_j}$. For each i, picking $\sigma_i \in G_{(i)} \setminus G_{(i+1)}$, we have $G_{(i)} = \langle \sigma_i, \sigma_{i+1}, ..., \sigma_n \rangle$. We denote by K_{i-1} the fixed field of $G_{(i)}$. Since K_i/K_{i-1} is an Artin–Schreier extension of degree p, there exists $X_i \in K_i$ such that $X_i^p - X_i \in K_{i-1}$, $\sigma_i(X_i) = X_i + 1$ and $v_{K_i}(X_i) = -b_{(i)}$ where $b_{(i)}$ is the ramification break number for K_i/K_{i-1}. We also have that $\gcd(b_{(i)}, p) = 1$. See [El09] for the

full detail.

It is known in [El09, §3, p.1195] that

$$\{b_{(0)}, b_{(1)}, ..., b_{(n)}\} = \{b_1, \ldots, b_m\}$$

is the set of ramification break numbers for K_n/K. Note that possibly $b_{(i)} = b_{(j)}$ although $i \neq j$. Also, Elder explains that each constant $b_{(i)}$ has a relationship with $b_{(n)}$ as

$$b_{(i)} \equiv b_{(n)} \pmod{p^{i+1}} \tag{2.4.1}$$

for $1 \leq i \leq n$. See [El09, §3, (2)].

Now, we are ready to present the special assumption. Define

$$\Delta_{i,j} = (\sigma_i - 1)(X_j).$$

Assumption 1. $\Delta_{i,j} \in K$ *for all* $0 \leq i, j \leq n$.

If Assumption 1 holds, Elder shows that K_n/K is elementary abelian and has the following property:

Proposition 2.4.1. *Let K_n/K be an extension defined above and satisfying Assumption 1. Let $\rho \in K_n$ be such that $v_{K_n}(\rho) \equiv b_{(n)} \pmod{p^{n+1}}$. Then, there exist $\Psi_0, \Psi_1, ..., \Psi_n \in K[G]$ such that*

$$v_{K_n}\left(\prod_{i=0}^{n} \Psi_i^{c_i} \rho\right) = v_{K_n}(\rho) + \sum_{i=0}^{n} c_i p^i b_{(n)}$$

for all $c_i \in \{0, 1, ..., p-1\}$.

Proof. See [El09, Proposition 3.3] □

Since $\gcd(b_{(n)}, p) = 1$, Proposition 2.4.1 implies that

$$\left\{ v_{K_n}\left(\prod_{i=0}^{n} \Psi_i^{c_i} \rho\right) : c_i = 0, 1, ..., p-1 \right\}$$

is a complete set of residues modulo p^{n+1}. Thus K_n/K admits a Galois scaffold by considering e.g. $b_{(n)}$ as an integer certificate.

Noticeably, the existence of Galois scaffolds in K_n/K depends on only Assumption 1. If there were no extensions satisfying Assumption 1, Proposition 2.4.1 would become vacuous. So, Elder constructed a class of field extensions, which he called 'one-dimensional elementary abelian extensions'. In fact, he also broadened that class of extensions to a larger class, near one-dimensional elementary abelian extensions, which still satisfy Assumption 1.

Definition 2.4.2. Let $K = k((T))$ be a local function field with perfect residue field k of characteristic $p > 0$. Let L/K be an abelian extension of degree p^{n+1}. Then, L is said to be a *one-dimensional elementary abelian extension* of K if there exists $x_0, x_1, ..., x_n$ satisfying the following conditions:

(i) $L = K(x_0, x_1, ..., x_n)$;

(ii) $x_i^p - x_i = \Omega_i^{p^n}\beta$ for some $\beta, \Omega_0 = 1, \Omega_1, ..., \Omega_n \in K$ where $v_K(\beta) = -b < 0$ with $\gcd(b, p) = 1$ and $v_K(\Omega_n) \leq ... \leq v_K(\Omega_1) \leq v_K(\Omega_0) = 0$;

(iii) If $v_K(\Omega_i) = ... = v_K(\Omega_j)$ for $i < j$, then the projections of $\Omega_i, ..., \Omega_j$ into $\Omega_i\mathfrak{O}_K/\Omega_i\mathfrak{P}_K$ are linearly independent over $\mathbb{F}_p$.

The extension L/K is called a *near one-dimensional elementary abelian extension* if $\beta, \Omega_0, ..., \Omega_n$ and x_0 are as above but for $1 \leq i \leq n$,

$$x_i^p - x_i = \Omega_i^{p^n}\beta + \epsilon_i$$

for some error terms $\epsilon_i \in K$ which satisfy

$$v_K(\epsilon_i) > v_K\left(\Omega_i^{p^n}\beta\right) + \frac{(p^n - 1)b}{p^n} - (p-1)\sum_{j=1}^{n-1} p^j v_K(\Omega_j).$$

Elder proves that near one-dimensional elementary abelian extensions satisfy Assumption 1. Thus, by Proposition 2.4.1, we have:

Theorem 2.4.3. *Any near one-dimensional elementary abelian extension possesses a Galois Scaffold.*

To close this subsection, it is worth mentioning that the set of ramification break numbers for a near one-dimensional elementary abelian extension L/K is

$$\{b_{(0)}, b_{(1)}, ..., b_{(n)}\}$$

where $b_{(i)} = b + p^n \sum_{j=1}^{i} p^j \left(v_K(\Omega_{j-1}) - v_K(\Omega_j)\right)$ [El09, p.1200].

2.4.2 Scaffolds

In [BCE], not only the definition of scaffolds, but the generalisation of integral Galois module structure is also included and studied.

Throughout this subsection, let L/K be a totally ramified extension of local fields of degree p^n where the residue field of K has characteristic $p > 0$. Let A be a K-algebra acting linearly on L with dimension p^n. For convenience, let us put $\mathbb{S}_m = \{0, 1, ..., m-1\}$. Note that for any $s \in \mathbb{S}_{p^n}$, we can write

$$s = \sum_{i=1}^{n} s_{(n-i)} p^{n-i} \quad \text{for some } s_{(n-i)} \in \mathbb{S}_p. \tag{2.4.2}$$

To present the definition of A-scaffold on L, it remains to set two notations $\mathfrak{b}$ and $\mathfrak{a}$. Let $b_1, ..., b_n$ be a sequence of integers relatively prime to p called *shift parameters*. With the expression of s in (2.4.2), we define a function $\mathfrak{b} : \mathbb{S}_{p^n} \to \mathbb{Z}$ by

$$\mathfrak{b}(s) = \sum_{i=1}^{n} s_{(n-i)} p^{n-i} b_i.$$

To make the map $\mathfrak{b}$ bijective, we define $\mathfrak{r} : \mathbb{Z} \to \mathbb{S}_{p^n}$ to be the residue function modulo p^n. In other words, $\mathfrak{r}(a) \equiv a \pmod{p^n}$ for any $a \in \mathbb{Z}$. Using the fact that b_i is relatively prime to p, we see that $\mathfrak{r} \circ \mathfrak{b}$ is a bijection on $\mathbb{S}_{p^n}$. In particular, the map $\mathfrak{r} \circ (-\mathfrak{b})$ is bijective. We denote the inverse of the map $\mathfrak{r} \circ (-\mathfrak{b})$ by $\mathfrak{a}$.

Definition 2.4.4 (A-scaffold on L)**.** Let $b_1, ..., b_n$, $\mathfrak{b}$ and $\mathfrak{a}$ be as above. Let $\mathfrak{c} \geq 1$. Then, an *A-scaffold on L* of precision $\mathfrak{c}$ with shift parameters $b_1, ..., b_n$ comprises

(i) The collection of $\{\lambda_t \in L : t \in \mathbb{Z}\}$ with $v_L(\lambda_t) = t$ such that $\lambda_{t_1}\lambda_{t_2}^{-1} \in K$ provided that $t_1 \equiv t_2 \pmod{p^n}$;

(ii) The collection of $\{\Psi_i \in A : 1 \leq i \leq n\}$ with $\Psi_i \cdot 1 = 0$ such that for any pair (i, t) there exists a unit $u_{i,t} \in \mathfrak{O}_K^\times$ making the following congruence modulo $\lambda_{t+p^{n-i}b_i}\mathfrak{P}_L^{\mathfrak{c}}$ hold:

$$\Psi_i \cdot \lambda_t \equiv \begin{cases} u_{i,t}\lambda_{t+p^{n-i}b_i} & \text{if } \mathfrak{a}(t)_{(n-i)} \geq 1, \\ 0 & \text{if } \mathfrak{a}(t)_{(n-i)} = 0. \end{cases}$$

If the congruence in (ii) is replaced by equality, we call *A-scaffold of precision ∞*.

Next, we explain how the concept of Galois scaffolds in [El09] agrees with the definition above after stating a theorem seen in the appendix A of [BCE]. Note that the theorem below is partially picked from the original version.

Theorem 2.4.5. *We use the notations as mentioned above and assume further that A is commutative. If, for each i, we have $\Psi_i \cdot 1 = 0$, $\Psi_i^p = 0$ and there exists $\rho \in L$ such that $v_L\left(\prod_{i=1}^{n} \Psi_i^{s_{n-i}} \cdot \rho\right) = v_L(\rho) + \mathfrak{b}(s)$ for all $s_i \in \mathbb{S}_p$, then L/K has an A-scaffold of precision ∞.*

Proof. See [BCE, Theorem A.1]. □

From the above theorem, we see that the Galois scaffold in a near one-dimensional elementary abelian extension L/K as in [El09] is a $K[G]$-scaffold of precision ∞ in the sense of Definition 2.4.4. This is because we can put the shift parameter b_i as the ramification break number $b_{(i)}$ of the extension K_i/K_{i-1} for $i = 0, 1, ..., n$ with the assistance of (2.4.1) i.e. $b_{(i)} \equiv b_{(n)} \pmod{p^{i+1}}$. Also, ρ is any element in L whose valuation is congruent to $b_{(n)}$ modulo p^{n+1}.

Moreover, it is simpler to show the existence of a scaffold by using Theorem 2.4.5 rather than by using Definition 2.4.4 directly.

We close this subsection by providing some references to see more examples of scaffolds. Byott and Elder show in [BE18] that Galois scaffolds can be found in both equicharacteristic and mixed characteristic local fields. Precisely, sufficient conditions for certain totally ramified extensions of equicharacteristic local fields to admit Galois scaffolds [BE18, Theorem 2.10] are provided. In the case of mixed characteristic local fields, see [BE18, Theorem 3.1 and Theorem 3.5]. Note that this paper contains only Galois scaffolds. To see examples of non-Galois scaffolds, one can consult [BCE, §5] and [Ko15]. However, the field extensions in both places are assumed to be inseparable, which is totally different from the setting in this thesis.

2.4.3 Integral Hopf-Galois Module Structure

This subsection can be understood as an application of scaffolds. To see the motivation for the study of integral Hopf-Galois module structure, we begin with some core materials in Galois module theory.

Theorem 2.4.6 (The Normal Basis Theorem)**.** *Let L/K be a finite Galois extension with Galois group $G = \{g_1, g_2, \ldots, g_m\}$. Then, there exists $x \in L$ such that $g_1(x), \ldots, g_m(x)$ form a basis for L/K.*

Proof. See [Un11, Proposition 10.5.1] □

The normal basis theorem is equivalent to the assertion that L is a free $K[G]$-module of rank 1. When L/K is an extension of global or local fields, algebraic

number theorists can naturally ask whether $\mathfrak{O}_L$ is a free module of rank 1 over $\mathfrak{O}_K[G]$.

Theorem 2.4.7 (Noether)**.** *Let L/K be a finite Galois extension of local fields with Galois group G. Then, the necessary and sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{O}_K[G]$ is that the extension is at most tamely ramified.*

Proof. See [Fr83, Theorem 3]. □

Clearly, Noether's theorem can answer such a question. Consequently, in the wild case, $\mathfrak{O}_K[G]$ is not a choice over which $\mathfrak{O}_L$ can be free. This leads to the study of the associated order in $K[G]$:

$$\mathfrak{A}_{K[G]} = \{\alpha \in K[G] : \alpha\mathfrak{O}_L \subset \mathfrak{O}_L\}.$$

We see from the definition above that the associated order can be easily defined in other Hopf-Galois structures on L/K by replacing $K[G]$ with any Hopf-Galois structures on the extension. Recall that, in this thesis, the classical Hopf-Galois structure $K[G]$ is excluded from the study. Moreover, the associated order is likely to be the most appropriate choice for the freeness question (see [Ch00, 12.5]). Now, we are ready to study integral Hopf-Galois module structure.

Let H be a Hopf algebra giving a Hopf-Galois structure on the extension L/K. Let $h \in \mathbb{Z}$ and consider the fractional ideal $\mathfrak{P}_L^h$ of the valuation ring $\mathfrak{O}_L$. Abusing the definition, we will call a fractional ideal an ideal although a fractional ideal is not necessarily an ideal. We define

$$\mathfrak{A} := \mathfrak{A}(h, H) = \left\{\alpha \in H : \alpha\mathfrak{P}_L^h \subseteq \mathfrak{P}_L^h\right\}$$

to be the *associated order* of the ideal $\mathfrak{P}_L^h$ in the Hopf algebra H. Then, we see that the ideal $\mathfrak{P}_L^h$ becomes an $\mathfrak{A}$-module. Next, one can naturally ask if the ideal $\mathfrak{P}_L^h$ is free over its associated order $\mathfrak{A}$.

Byott, Childs and Elder can answer such a question by giving a necessary condition for $\mathfrak{P}_L^h$ to be free over $\mathfrak{A}$ provided that a scaffold exist on the field extension. This condition is also sufficient if the precision is high enough.

In order to see the condition, we have to put a partial order $\preceq$ on $\mathbb{S}_{p^n}$ based upon the expression in (2.4.2). For $s, t \in \mathbb{S}_{p^n}$, we write $s \preceq t$ if $s_{(n-i)} \leq t_{(n-i)}$ for all $i = 1, 2, \ldots, n$.

Assume that L/K admits an H-scaffold of precision $\mathfrak{c}$. Fix an ideal $\mathfrak{P}_L^h$ and define $\mathbb{S}_{p^n}(h) = \{t \in \mathbb{Z} : h \leq t < h + p^n\}$. Note that $\mathbb{S}_{p^n}(0) = \mathbb{S}_{p^n}$. Let $\mathscr{B}$ be an integer such that $\mathscr{B} \in \mathbb{S}_{p^n}(h)$ and $\mathfrak{a}(\mathfrak{r}(\mathscr{B})) = p^n - 1$. Then, the relationship of following maps on $\mathbb{S}_{p^n}$ plays a major part in determining the freeness of the ideal $\mathfrak{P}_L^h$:

$$\mathfrak{d}(s) = \left\lfloor \frac{\mathfrak{b}(s) + \mathscr{B} - h}{p^n} \right\rfloor \tag{2.4.3}$$

and
$$\mathfrak{w}(s) = \min\{\mathfrak{d}(s + j) - \mathfrak{d}(j) : j \in \mathbb{S}_{p^n},\ j \preceq p^n - 1 - s\} \tag{2.4.4}$$

for any $s \in \mathbb{S}_{p^n}$.

Theorem 2.4.8. *Assume that L/K possesses an H-scaffold of precision $\mathfrak{c}$. Let $\mathfrak{P}_L^h$ be an ideal of $\mathfrak{O}_L$.*

(i) If $\mathfrak{c} > \max(\mathscr{B} - h, 1)$ and $\mathfrak{w}(s) = \mathfrak{d}(s)$ for all $s \in \mathbb{S}_{p^n}$, then $\mathfrak{P}_L^h$ is free over $\mathfrak{A}$.

(ii) If $\mathfrak{c} \geq p^n + \mathscr{B} - h$, then $\mathfrak{P}_L^h$ is free over $\mathfrak{A}$ iff $\mathfrak{w}(s) = \mathfrak{d}(s)$ for all $s \in \mathbb{S}_{p^n}$.

Proof. See [BCE, Theorem 3.1]. □

Remarkably, having a scaffold of high precision in hand, we can answer the question of the freeness of ideals over their associated orders easily.

Chapter 3

Hopf-Galois Structures on $C_p \times C_p$ Extensions in Characteristic p

We recall in Theorem 3.1.1 below the description of the Hopf-Galois structures on an elementary extension L/K of degree p^2. There are precisely p^2 such Hopf-Galois structures, with $p-1$ non-classical Hopf-Galois structures associated to each of the $p+1$ subgroups T of order p in $G = \mathrm{Gal}(L/K)$. This applies in particular when L/K is a near one-dimensional elementary abelian extension of degree p^2.

After knowing all the Hopf-Galois structures on L/K, a near one-dimensional elementary abelian extension, we introduce a unified language to carry out certain algebraic calculations in all the non-classical Hopf-Galois structures simultaneously. Our extension L/K will typically have two distinct ramification break numbers. When we bring arithmetic information (the valuations of particular elements) into play, we will need to treat the non-classical Hopf-Galois structures for which T is the 'special' subgroup of order p occurring in the ramification filtrations separately from the rest. We end this chapter by introducing two convenient generators for each Hopf algebra arising in the non-classical Hopf-Galois structures.

3.1 The Set-Up

Theorem 3.1.1. *Let L/K be a Galois extension of degree p^2 with elementary abelian Galois group G. Let T be one of the $p+1$ subgroups of G of order p. Let $T = \langle \tau \rangle$ for some $\tau \in G$. Let $\sigma \in G$ be such that $G = \langle \sigma, \tau \rangle$ and $\sigma^p = 1_G$. We fix $d \in \{0, 1, ..., p-1\}$. Then, we have*

(i) There are well-defined elements $\rho, \eta \in Perm(G)$ determined by

$$\begin{aligned} \rho(\sigma^k \tau^l) &= \sigma^k \tau^{l-1} \\ \eta(\sigma^k \tau^l) &= \sigma^{k-1} \tau^{l+(k-1)d} \qquad \text{for } k, l \in \mathbb{Z}, \end{aligned}$$

(ii) From (i), we have that $\rho^p = 1$ and $\rho\eta = \eta\rho$. Furthermore,

$$\eta^r(\sigma^k \tau^l) = \sigma^{k-r} \tau^{l+drk-dr(r+1)/2} \quad \text{for } r \in \mathbb{Z};$$

(iii) If $p \neq 2$ or $d \neq 1$, then $\eta^p = 1$;

(iv) Taking $N = N_{T,d} = \langle \rho, \eta \rangle$, we have that N is a regular subgroup of Perm(G) of order p^2 normalised by $\lambda(G)$, and $N \cong G$ unless $p = 2$, $d = 1$;

(v) If $d = 0$, then N gives us the classical Hopf-Galois structure;

(vi) There are p^2 Hopf-Galois structures on L/K.

Proof. See [By96] □

The scope of this thesis is to investigate non-classical Hopf-Galois structures on near one-dimensional elementary abelian extensions of degree p^2, $p \geq 3$. We recall from Definition 2.4.2 that in our situation $K = k((T))$ and L/K is a near one-dimensional elementary abelian extension of degree p^2 with Galois group G. Note that the reason why we exclude $p = 2$ is due to Theorem 3.1.1(iii). Then, there exist $x_0, x_1 \in L$ such that $L = K(x_0, x_1)$ with the properties that

$$x_0^p - x_0 = \beta \quad \text{and} \quad x_1^p - x_1 = \Omega^p \beta + \epsilon \tag{3.1.1}$$

for some $\beta, \Omega, \epsilon \in K$. The error term ϵ satisfies

$$v_K(\epsilon) > v_K\left(\Omega^p \beta\right) + \frac{(p-1)b}{p}. \tag{3.1.2}$$

We also have $v_K(\beta) = -b < 0$ and $p \nmid b$. We denote by $w := -v_K(\Omega)$ where $w \geq 0$. Recall that if $w = 0$, then 1 and Ω must satisfy the independence condition (iii) in Definition 2.4.2. Since $G \cong C_p \times C_p$, we fix $\omega \in G$ be such that

$$\omega(x_0) = x_0 + 1 \quad \text{and} \quad \omega(x_1) = x_1. \tag{3.1.3}$$

Then there exists $\nu \in G$ such that

$$\nu(x_1) = x_1 + 1 \quad \text{and} \quad \nu(x_0) = x_0. \tag{3.1.4}$$

We also have $\omega^p = \nu^p = 1$ and thus $G = \langle \nu, \omega \rangle$.

3.2 Unified Language

Since there are $p+1$ subgroups of order p in $G \cong C_p \times C_p$, there are $p+1$ choices for T in Theorem 3.1.1. Explicitly, they are $\langle \omega \rangle, \langle \nu\omega \rangle, \langle \nu^2\omega \rangle, \ldots, \langle \nu^{p-1}\omega \rangle, \langle \nu \rangle$. In order to study all the $p^2 - 1$ non-classical Hopf-Galois structures on L/K simultaneously, we set a pack of parameters called 'unified language' to work with.

Before providing a dictionary between unified language and other Hopf-Galois structures, we distinguish subgroups of order p in G by the ramification break numbers for L/K. In [El09], it is known that the set of ramification break numbers of L/K is $\{b, b + p^2 w\}$. However, w is allowed to be 0. If it is the case, the extension has only one break; otherwise there are two. In particular, for the latter case, the subfield $K(x_0)$ (over K) has the ramification break number b; whereas the other subfields have the ramification break number $b + p^2 w$. With this reason, we say that the subgroup $\langle \nu \rangle$ of G is *special* as it corresponds to the distinguished

subfield $K(x_0)$ of L. The other subgroups of order p in G are called *non-special*.

However, when $w = 0$, or in other words, L/K has only one ramification break number, the word 'special' does not literally mean special but only refer to the subgroup $\langle\nu\rangle$ not the others.

Then, Table 1 introduces all the notations used in this thesis as well as the dictionary between unified language and Hopf-Galois structures arising from the special/non-special subgroups.

Unified language	HGS arising from $\langle\nu^{-i}\omega\rangle$	HGS arising from $\langle\nu\rangle$
β_1	β	$\Omega^p\beta$
Ω_1	$\Omega + i$	Ω^{-1}
$\overline{\Omega}$	$(\Omega + i)^p\beta + \epsilon$	β
τ	$\nu^{-i}\omega$	ν
σ	ν	ω
A	$ix_0 + x_1$	x_0
B	$x_0 - (\Omega + i)^{-1}(ix_0 + x_1)$	$x_1 - \Omega x_0$

Table 1: Dictionary between unified language and other Hopf-Galois structures arising from various subgroups of G.

The dictionary is used for translating parameters in Hopf-Galois structures into unified language and vice versa. For example, if we write

$$\tau\left(A - \beta_1\right)$$

in unified language, it means we write

$$\nu^{-i}\omega\left((ix_0 + x_1) - \beta\right)$$

in Hopf-Galois structures arising from subgroup $\langle\nu^{-i}\omega\rangle$ and means

$$\nu(x_0 - \Omega^p\beta)$$

in Hopf-Galois structures arising from the special subgroup $\langle\nu\rangle$.

Moreover, with this dictionary, we can translate some algebraic relations, which are required in this study (Proposition 3.2.1 and 3.2.2), from one language to another. This allows us to work with all of them at a time via unified language.

For the unified study, we set $L[N_{T,d}]^G$ (or sometimes just $L[N]^G$) as a delegate of all the non-classical Hopf-Galois structures on L/K. Bear in mind that T is any of the following subgroups

$$\langle\omega\rangle, \langle\nu\omega\rangle, \langle\nu^2\omega\rangle, \ldots, \langle\nu^{p-1}\omega\rangle, \langle\nu\rangle$$

and $d \in \{1, 2, ..., p-1\}$. Also, all the parameters are written in unified language. Once the interpretation is needed, we use Table 1 to translate back into the context of the considered Hopf-Galois structure.

Proposition 3.2.1. *In the Hopf-Galois structure $L[N_{T,d}]^G$, the following algebraic relations hold:*

(i) $\tau(A) = A$,

(ii) $\sigma(A) = A + 1$,

(iii) $A^p - A = \overline{\Omega}$,

(iv) $\tau(B) = B + 1$,

(v) $\sigma(B) = B - \Omega_1^{-1}$.

Proof. Refer to (3.1.3) and (3.1.4). For the Hopf-Galois structure arising from $\langle\nu^{-i}\omega\rangle$, we have that

(i) $\nu^{-i}\omega(ix_0 + x_1) = \nu^{-i}(ix_0 + x_1 + i) = ix_0 + x_1$,

(ii) $\nu(ix_0 + x_1) = (ix_0 + x_1) + 1$,

(iii) $(ix_0 + x_1)^p - (ix_0 + x_1) = (x_1^p - x_1) + i(x_0^p - x_0) = (\Omega + i)^p\beta + \epsilon$ by (3.1.1),

(iv) $\nu^{-i}\omega\left(x_0-(\Omega+i)^{-1}(ix_0+x_1)\right)=x_0-(\Omega+i)^{-1}(ix_0+x_1)+1$,

(v) $\nu\left(x_0-(\Omega+i)^{-1}(ix_0+x_1)\right)=x_0-(\Omega+i)^{-1}(ix_0+x_1)-(\Omega+i)^{-1}$.

In terms of the other, we have

(i) $\nu(x_0)=x_0$,

(ii) $\omega(x_0)=x_0+1$,

(iii) $x_0^p-x_0=\beta$,

(iv) $\nu(x_1-\Omega x_0)=(x_1-\Omega x_0)+1$,

(v) $\omega(x_1-\Omega x_0)=(x_1-\Omega x_0)-\Omega$.

□

Previously, we proceeded from algebraic viewpoint. Now, it is time to adopt an arithmetic one. Due to (3.1.1) and (3.1.2), we have

$$pv_L(x_0)=-p^2b \text{ and } pv_L(x_1)=-p^3w-p^2b.$$

Hence, $v_L(x_0)=-pb$ and $v_L(x_1)=-p^2w-pb$. This suggests that x_0,x_1 are not good objects to work with as they have the same valuation modulo p.

It is found that A,B defined as in the dictionary Table 1 are worth working with due to their arithmetic property.

Proposition 3.2.2. *We have*

- $v_L(A)=-p^2w\delta_T-pb$; *and*
- $v_L(B)=-p^2w(1-\delta_T)-b$

where $\delta_T=\begin{cases}1 & \text{if } T \text{ is non-special;}\\ 0 & \text{otherwise.}\end{cases}$

In particular, $\{A^iB^j:0\le i,j\le p-1\}$ *forms a basis for* L/K *in any Hopf-Galois structure.*

Proof. In Hopf-Galois structures arising from non-special subgroups, we have

$$A^p - A = (\Omega + i)^p \beta + \epsilon.$$

If $v_K(\Omega) < 0$, then, by (3.1.2), we have $v_L\left((\Omega + i)^p \beta + \epsilon\right) = v_L(\Omega^p \beta) = -p^3 w - p^2 b$. If $v_K(\Omega) = 0$, then, by Definition 2.4.2(iii), we have $v_L\left((\Omega + i)^p \beta + \epsilon\right) = v_L(\beta) = -p^2 b$. Hence, in the both cases, we have $v_L(A) = -p^2 w - pb$.

It is easy to see $v_L(A) = -pb$ in Hopf-Galois structures arising from the special subgroup as $A = x_0$.

The computation for $v_L(B)$ is a bit more complicated as shown below.

• *Hopf-Galois structures arising from* $\langle \nu^{-i} \omega \rangle$

$$\begin{aligned} B^p - B &= (x_0^p - x_0) - (\Omega + i)^{-p}(ix_0 + x_1)^p + (\Omega + i)^{-1}(ix_0 + x_1) \\ &= \beta - (\Omega + i)^{-p}\left((ix_0 + x_1)^p - (ix_0 + x_1)\right) - \left((\Omega + i)^{-p} - (\Omega + i)^{-1}\right)(ix_0 + x_1) \\ &= \beta - (\Omega + i)^{-p}\left((\Omega + i)^p \beta + \epsilon\right) - \left((\Omega + i)^{-p} - (\Omega + i)^{-1}\right)(ix_0 + x_1) \\ &= -(\Omega + i)^{-p}\epsilon - \left((\Omega + i)^{-p} - (\Omega + i)^{-1}\right)(ix_0 + x_1). \end{aligned}$$

If $v_K(\Omega) < 0$, by (3.1.2), we have

$$v_L\left((\Omega + i)^{-p}\,\epsilon\right) = p^3 w + p^2 v_K(\epsilon) > -pb = v_L\left(\left((\Omega + i)^{-p} - (\Omega + i)^{-1}\right)(ix_0 + x_1)\right).$$

This gives us $pv_L(B) = -pb$ and hence $v_L(B) = -b$. If $v_K(\Omega) = 0$, we consider that $(\Omega + i)^{-p} - (\Omega + i)^{-1} = (\Omega + i)^{-p}\left(1 - (\Omega + i)^{p-1}\right)$. Due to the fact that the polynomial $T^{p-1} - 1$ splits in $\mathbb{F}_p$ and the third condition of one-dimensional elementary abelian extensions, we have $v_L\left(1 - (\Omega + i)^{p-1}\right) = 0$ and hence

$$v_L\left(\left((\Omega + i)^{-p} - (\Omega + i)^{-1}\right)(ix_0 + x_1)\right) = -pb.$$

As far as ϵ is concerned, we have

$$v_L\left((\Omega + i)^{-p}\epsilon\right) = p^3 w + v_L(\epsilon) > p^3 w - p^3 w - pb = -pb.$$

Thus, $v_L(B) = -b$

• *Hopf-Galois structures arising from* $\langle\nu\rangle$

$$\begin{aligned} B^p - B &= (x_1^p - x_1) - \Omega^p(x_0^p - x_0) - (\Omega^p - \Omega)x_0 \\ &= (\Omega^p\beta + \epsilon) - \Omega^p\beta - (\Omega^p - \Omega)x_0 \\ &= \epsilon - (\Omega^p - \Omega)x_0. \end{aligned}$$

Then, we compute

$$v_L\left((\Omega^p - \Omega)\, x_0\right) = v_L\left(\Omega\left(\Omega^{p-1} - 1\right) x_0\right) = -p^3w - pb.$$

Since $v_L(\epsilon) > -p^3w - pb$, we have that $v_L(B)$ is determined by the term $(\Omega^p - \Omega)x_0$ Hence, we have $pv_L(B) = -p^3w - pb$ implying that $v_L(B) = -p^2w - b$ in Hopf-Galois structures arising from the special subgroup.

Thus, for every non-classical Hopf-Galois structure, $v_L(A) \not\equiv v_L(B) \pmod{p}$. In particular, $\{v_L(A^iB^j) : 0 \le i, j \le p-1\}$ is a complete set of residues modulo p^2. As a result, $\{A^iB^j : 0 \le i, j \le p-1\}$ forms a basis for L/K. □

Remark. We draw a table below recording the valuations of significant terms in any Hopf-Galois structure. According to the table, we see that if Ω is a unit (i.e. $w = 0$), $v_L(A)$ (resp. $v_L(B)$) is the same in all non-classical Hopf-Galois structures.

Valuation in L of	HGS arising from $\langle\nu^{-i}\omega\rangle$	HGS arising from $\langle\nu\rangle$
Ω_1	$-p^2w$	p^2w
β_1	$-p^2b$	$-p^3w - p^2b$
$\overline{\Omega}$	$-p^3w - p^2b$	$-p^2b$
A	$-p^2w - pb$	$-pb$
B	$-b$	$-p^2w - b$

Table 2: Valuation table.

3.3 Shapes of Hopf algebras on L/K

Before describing $L[N_{T,d}]^G$, we need to know how G acts on $N = \langle \rho, \eta \rangle$. Bear in mind that no matter what subgroup we pick for T and what value for d, we work with unified language instead thanks to Proposition 3.2.1. Hence, $T = \langle \tau \rangle$, $G = \langle \sigma, \tau \rangle$ and $L = K(A, B)$.

Proposition 3.3.1. *We have*
(i) $\tau^m \cdot \rho^a \eta^b = \rho^a \eta^b$
(ii) $\sigma^n \cdot \rho^a \eta^b = \rho^{a+dbn} \eta^b$.

Proof. (i) By Proposition 2.2.6, we have $\tau^m \cdot \rho^a \eta^b = \lambda(\tau^m)\rho^a \eta^b \lambda(\tau^{-m})$. Then, by Theorem 3.1.1, for any $u, v \in \mathbb{S}_p$, we have

$$\begin{aligned}
\lambda(\tau^m)\rho^a \eta^b \lambda(\tau^{-m})(\sigma^u \tau^v) &= \lambda(\tau^m)\rho^a \eta^b \left(\sigma^u \tau^{v-m}\right) \\
&= \lambda(\tau^m)\rho^a \left(\sigma^{u-b} \tau^{v-m+dbu-db(b+1)/2}\right) \\
&= \sigma^{u-b} \tau^{v+dbu-db(b+1)/2-a} \\
&= \rho^a \eta^b (\sigma^u \tau^v).
\end{aligned}$$

(ii) Similarly to (i), we have

$$\begin{aligned}
\lambda(\sigma^n)\rho^a \eta^b \lambda(\sigma^{-n})(\sigma^u \tau^v) &= \sigma^{u-b} \tau^{v+dbu-db(b+1)/2-dbn-a} \\
&= \rho^{a+dbn} \eta^b (\sigma^u \tau^v).
\end{aligned}$$

□

Proposition 3.3.2. *We make the convention that* $0^0 = 1$. *Taking* $\Lambda_0 = \rho - 1$ *and* $\Lambda_1 = -\sum_{i=0}^{p-1} (-1)^i A^{p-i-1} \sum_{j=0}^{p-1} j^i \rho^{dj} \eta - 1$, *we have*

(i) $\Lambda_0, \Lambda_1 \in L[N]^G$;

(ii) $\Lambda_0^p = \Lambda_1^p = 0$; *and*

(iii) $L[N]^G = K[\Lambda_0, \Lambda_1]$.

Proof. (i) By Proposition 3.3.1(i) and Proposition 3.2.1(i), we have

$$\tau \cdot \Lambda_0 = \Lambda_0 \quad \text{and} \quad \tau \cdot \Lambda_1 = \Lambda_1.$$

By Proposition 3.3.1(ii), we have $\sigma \cdot \Lambda_0 = \Lambda_0$ implying that $\Lambda_0 \in L[N]^G$.

Before we see $\Lambda_1 \in L[N]^G$, it is worth recalling that $0^0 = 1$ and noting that $\binom{p-1}{i} = (-1)^i$. The latter is obtained from the so-called Wilson's theorem and the fact that we work over $\mathbb{F}_p$. Then, we compute

$$\begin{aligned}
\Psi := -\Lambda_1 - 1 &= \sum_{i=0}^{p-1} (-1)^i A^{p-i-1} \sum_{j=0}^{p-1} j^i \rho^{dj} \eta \\
&= \sum_{i=0}^{p-1} \binom{p-1}{i} A^{p-i-1} \sum_{j=0}^{p-1} j^i \rho^{dj} \eta \\
&= \sum_{i=0}^{p-1} \binom{p-1}{i} A^{p-i-1} \left(0^i \eta + \sum_{j=1}^{p-1} j^i \rho^{dj} \eta \right) \\
&= A^{p-1}\eta + \sum_{i=0}^{p-1} \sum_{j=1}^{p-1} \binom{p-1}{i} A^{p-1-i} j^i \rho^{dj} \eta \\
&= A^{p-1}\eta + \sum_{j=1}^{p-1} (A+j)^{p-1} \rho^{dj} \eta \\
&= \sum_{j=0}^{p-1} (A+j)^{p-1} \rho^{dj} \eta.
\end{aligned}$$

Then, by Proposition 3.3.1(ii) and Proposition 3.2.1(ii), we have

$$\begin{aligned}
\sigma \cdot \Psi &= \sigma \cdot \left(\sum_{j=0}^{p-1} (A+j)^{p-1} \rho^{dj} \eta \right) \\
&= \sum_{j=0}^{p-1} \left(A + (j+1)\right)^{p-1} \rho^{d(j+1)} \eta \\
&= \sum_{j=0}^{p-1} (A+j)^{p-1} \rho^{dj} \eta = \Psi.
\end{aligned}$$

Thus, $\sigma \cdot \Lambda_1 = \Lambda_1$.

(ii) It is obvious from Theorem 3.1.1(ii) that $\Lambda_0^p = 0$. To see that $\Lambda_1^p = 0$, we compute:

$$\begin{aligned}\left(\sum_{j=0}^{p-1} j^i \rho^{dj}\eta\right)^p &= \left(0^i\eta + \sum_{j=1}^{p-1} j^i \rho^{dj}\eta\right)^p \\ &= 0^i + \sum_{j=1}^{p-1} j^i \\ &= \begin{cases} 1 + \displaystyle\sum_{j=1}^{p-1} j^i & \text{if } i = 0; \\ \displaystyle\sum_{j=1}^{p-1} j^i & \text{if } i = 1, \ldots, p-1. \end{cases}\end{aligned}$$

Since

$$\sum_{j=1}^{p-1} j^i \equiv \begin{cases} -1 \pmod p & \text{if } p-1 \mid i \\ 0 \pmod p & \text{otherwise,} \end{cases}$$

we have

$$\left(\sum_{j=0}^{p-1} j^i \rho^{dj}\eta\right)^p = \begin{cases} 0 & \text{if } i = 0, 1, \ldots, p-2; \\ -1 & \text{if } i = p-1. \end{cases}$$

Thus,

$$\Psi^p = \sum_{i=0}^{p-1} (-1)^i A^{p(p-i-1)} \left(\sum_{j=0}^{p-1} j^i \rho^{dj}\eta\right)^p = (-1)^{p-1}(-1) = -1.$$

and hence $\Lambda_1^p = 0$.

(iii) From (i) and (ii), we see that $K[\Lambda_0, \Lambda_1]$ is a K-subalgebra of $L[N]^G$ of dimension p^2. Therefore, $K[\Lambda_0, \Lambda_1] = L[N]^G$. □

Remark. Λ_0 and Λ_1 are well-behaved generators since, by Proposition 3.3.2(ii), we see that they satisfy one third of conditions in Theorem 2.4.5. Moreover, we can shortly show that $\Lambda_0 \cdot 1 = \Lambda_1 \cdot 1 = 0$ (see Proposition 4.1.1(ii)).

Chapter 4

Actions of Hopf Algebras on L

To master the $p^2 - 1$ non-classical Hopf-Galois structures on L/K, we provide formulae enabling us to compute the actions of the two generators Λ_0 and Λ_1 on L. Bear in mind that in this chapter we work only in unified language. Unfortunately, the formulae are quite difficult to work with. We need some tools making them tractable. It is found that colexicographical ordering can help us develop tools by extracting only essential information from the intricate formulae.

4.1 Formulae for Actions of Λ_0 and Λ_1 on L

Recall that in the previous chapter we have the Hopf algebra $L[N_{T,d}]^G$ where $G = \langle \tau, \sigma \rangle$ and $N_{T,d} = \langle \rho, \eta \rangle$. Let us occasionally write $L[N]^G$ for short. Now, we are in a position to translate the action of it on L.

Proposition 4.1.1. *(i)* $\rho^{-k}(1_G) = \tau^k$ *and* $\eta^{-k}(1_G) = \sigma^k \tau^{\frac{-dk(k-1)}{2}}$,
(ii) $\Lambda_0 \cdot 1 = \Lambda_1 \cdot 1 = 0$.

Proof. (i) follows immediately from Theorem 3.1.1(i) and (ii).

(ii) Recall (2.2.1). From (i), we see that

$$\begin{aligned}\Lambda_0 \cdot 1 &= (\rho - 1) \cdot 1 \\ &= (\rho)^{-1}(1_G)(1) - 1 \\ &= \tau(1) - 1 \\ &= 0.\end{aligned}$$

For the other identity, we calculate as shown below:

$$\begin{aligned}\Lambda_1 \cdot 1 &= \left(-\sum_{i=0}^{p-1}(-1)^i A^{p-i-1} \sum_{j=0}^{p-1} j^i \rho^{dj} \eta - 1 \right) \cdot 1 \\ &= -\sum_{i=0}^{p-1}(-1)^i A^{p-i-1} \sum_{j=0}^{p-1} j^i (\rho^{dj}\eta)^{-1}(1_G)(1) - 1 \\ &= -\sum_{i=0}^{p-1}(-1)^i A^{p-i-1} \sum_{j=0}^{p-1} j^i \sigma\tau^{dj}(1) - 1 \\ &= -\sum_{i=0}^{p-1}(-1)^i A^{p-i-1} \sum_{j=0}^{p-1} j^i - 1 = -(-1) - 1 = 0.\end{aligned}$$

□

In this thesis, there are two useful ways of expressing the action of $L[N]^G$ on L. Of course, one way is writing in terms of $A^r B^s$ for $0 \leq r, s \leq p-1$, whereas the other is in terms of $A^r B^s$ for $r \geq 0$ (with $r \geq p$ allowed) and $0 \leq s \leq p-1$. The latter will be applied only when we want to count the degree of A in $\Lambda_1^i A^r B^s$.

Due to Proposition 3.2.1, we can prove Proposition 4.1.2. Moreover, the proposition can be translated into every non-classical Hopf-Galois structure on L/K since every algebraic action done in the proof is contained in Proposition 3.2.1.

Proposition 4.1.2. *In the Hopf-Galois structure $L[N_{T,d}]^G$, for $r \geq 0$ and $0 \leq s \leq p-1$, we have*

(i) $\Lambda_0 A^r B^s = A^r \left[\sum_{u=1}^{s} \binom{s}{u} B^{s-u} \right]$; *and*

(ii)

$$\Lambda_1 A^r B^s = \sum_{u=0}^{s}\sum_{t=0}^{r}\binom{s}{u}\binom{r}{t}(-d)^u A^{r-t+u}(B-\Omega_1^{-1})^{s-u} + \sum_{v=0}^{r}\binom{r}{v}\delta_{s,p-1}A^v - A^r B^s. \tag{4.1.1}$$

For $0 \le r, s \le p-1$, we have

$$\begin{aligned}\Lambda_1 A^r B^s = &\sum_{\substack{u+v<p\\ u\le s, v\le r}}(-d)^u\binom{r}{v}\binom{s}{u}A^{u+v}(B-\Omega_1^{-1})^{s-u}\\ &+\sum_{\substack{u+v\ge p\\ u\le s, v\le r}}(-d)^u\binom{r}{v}\binom{s}{u}A^{u+v-p+1}(B-\Omega_1^{-1})^{s-u}\\ &+\sum_{\substack{u+v\ge p\\ u\le s, v\le r}}(-d)^u\binom{r}{v}\binom{s}{u}\overline{\Omega}A^{u+v-p}(B-\Omega_1^{-1})^{s-u}\\ &+\sum_{v=0}^{r}\binom{r}{v}\delta_{s,p-1}A^v - A^r B^s. \end{aligned}\tag{4.1.2}$$

Note that (4.1.1) expresses $\Lambda_1 A^r B^s$ in terms of $A^i B^j$ for $i \ge 0$ (with $i \ge p$ allowed) and $0 \le j \le p-1$; whereas (4.1.2) expresses in terms of the basis $A^i B^j$ for $0 \le i, j \le p-1$.

Proof. (i) By Proposition 4.1.1(i) and Proposition 3.2.1(i) and (iv), we have

$$\begin{aligned}\Lambda_0 A^r B^s &= (\rho - 1)\cdot A^r B^s\\ &= (\tau - 1)\,(A^r B^s)\\ &= A^r(B+1)^s - A^r B^s\\ &= A^r\left[\sum_{u=1}^{s}\binom{s}{u}B^{s-u}\right].\end{aligned}$$

(ii) For simplicity, we will work with $\Psi := -\Lambda_1 - 1 = \sum_{i=0}^{p-1}(-1)^i A^{p-1-i}\sum_{j=0}^{p-1} j^i \rho^{dj}\eta$.

Then, we have

$$\begin{aligned}
\Psi A^r B^s &= \sum_{i=0}^{p-1}(-1)^i A^{p-1-i}\sum_{j=0}^{p-1} j^i \rho^{dj}\eta\cdot(A^rB^s)\\
&= \sum_{i=0}^{p-1}(-1)^i A^{p-1-i}\sum_{j=0}^{p-1} j^i \sigma\tau^{dj}(A^rB^s) \qquad \text{(by Proposition 4.1.1(i))}\\
&= \sum_{i=0}^{p-1}(-1)^i A^{p-1-i}\sum_{j=0}^{p-1} j^i \tau^{dj}(A+1)^r(B-\Omega_1^{-1})^s\\
&\qquad\qquad \text{(by Proposition 3.2.1(ii) and(v))}\\
&= \sum_{i=0}^{p-1}(-1)^i A^{p-1-i}\sum_{j=0}^{p-1} j^i (A+1)^r\left((B-\Omega_1^{-1})+dj\right)^s\\
&\qquad\qquad \text{(by Proposition 3.2.1(i) and (iv))}\\
&= (A+1)^r\sum_{i=0}^{p-1}(-1)^i A^{p-1-i}\sum_{j=0}^{p-1} j^i \left((B-\Omega_1^{-1})+dj\right)^s\\
&= (A+1)^r\sum_{i=0}^{p-1}(-1)^i A^{p-1-i}\sum_{j=0}^{p-1} j^i \sum_{u=0}^{s}\binom{s}{u}(B-\Omega_1^{-1})^{s-u}(dj)^u\\
&= (A+1)^r\sum_{i=0}^{p-1}(-1)^i A^{p-1-i}\sum_{u=0}^{s}\binom{s}{u}(B-\Omega_1^{-1})^{s-u}d^u\sum_{j=0}^{p-1} j^{i+u}.
\end{aligned}$$

We see that, for each u, the final sum vanishes unless $i+u$ is divisible by $p-1$ and $i+u>0$. Thus, if $u\in\{0,1,...,p-2\}$, i must be $p-1-u$; but if $u=p-1$ then i can be both 0 and $p-1$. It follows that

$$\begin{aligned}
\Psi A^r B^s &= -(A+1)^r\left[\sum_{u=0}^{s}\binom{s}{u}(-Ad)^u(B-\Omega_1^{-1})^{s-u}+\delta_{s,p-1}d^{p-1}\right]\\
&= \sum_{u=0}^{s}\sum_{v=0}^{r}\binom{s}{u}\binom{r}{v}(-1)^{u+1}d^uA^{u+v}(B-\Omega_1^{-1})^{s-u}-\sum_{v=0}^{r}\binom{r}{v}\delta_{s,p-1}d^{p-1}A^v.
\end{aligned}$$

Thus, we have

$$\Lambda_1 A^r B^s = \sum_{u=0}^{s}\sum_{v=0}^{r}\binom{s}{u}\binom{r}{v}(-d)^uA^{u+v}(B-\Omega_1^{-1})^{s-u}+\sum_{v=0}^{r}\binom{r}{v}\delta_{s,p-1}A^v-A^rB^s$$

or, putting $t = r - v$,

$$\Lambda_1 A^r B^s = \sum_{u=0}^{s} \sum_{t=0}^{r} \binom{s}{u} \binom{r}{t} (-d)^u A^{r-t+u} (B - \Omega_1^{-1})^{s-u} + \sum_{v=0}^{r} \binom{r}{v} \delta_{s,p-1} A^v - A^r B^s.$$

This proves (4.1.1).

Next, we prove (4.1.2). Recall that, here, $0 \leq r, s \leq p-1$. As $u+v$ can be greater than $p-1$, we expand the formula. Recall from Proposition 3.2.1(iii) that

$$A^p = A + \overline{\Omega}.$$

If $u + v \geq p$, then $A^{u+v} = A^{u+v-p+1} + A^{u+v-p}\overline{\Omega}$. Therefore, we have

$$\begin{aligned}
\Lambda_1 A^r B^s = & \sum_{\substack{u+v<p \\ u\leq s, v\leq r}} (-d)^u \binom{r}{v} \binom{s}{u} A^{u+v} (B - \Omega_1^{-1})^{s-u} \\
& + \sum_{\substack{u+v\geq p \\ u\leq s, v\leq r}} (-d)^u \binom{r}{v} \binom{s}{u} A^{u+v-p+1} (B - \Omega_1^{-1})^{s-u} \\
& + \sum_{\substack{u+v\geq p \\ u\leq s, v\leq r}} (-d)^u \binom{r}{v} \binom{s}{u} \overline{\Omega} A^{u+v-p} (B - \Omega_1^{-1})^{s-u} \\
& + \sum_{v=0}^{r} \binom{r}{v} \delta_{s,p-1} A^v - A^r B^s.
\end{aligned}$$

Note that since $0 \leq r, s \leq p-1$, we have $u + v - p < u + v - p + 1 \leq p - 1$. This proves (4.1.2). □

Due to the identity $A^p = A + \overline{\Omega}$, there are two ways to express terms in $\Lambda_1 A^r B^s$. The first way is to write in terms of $A^i B^j$ for $i \geq 0$ (with $i \geq p$ allowed) and $0 \leq j \leq p-1$. Note that, in this way, the coefficients of $A^i B^j$ are in $\mathbb{F}_p\left[\Omega_1^{-1}\right]$ without involving $\overline{\Omega}$ (as in (4.1.1)). The other is in terms of $A^i B^j$ for $0 \leq i, j \leq p-1$ but with coefficients involving $\overline{\Omega}$ (as in (4.1.2)). The identity also makes 'degree in A' not well-defined. To avoid confusion, let us declare here that we express terms in $\Lambda_1 A^r B^s$ as in (4.1.1) only in Proposition 4.2.7, the whole of Section 4.3 and the whole of Chapter 7. Hence, apart from these places, we express terms in $\Lambda_1 A^r B^s$

as in (4.1.2). This means that each way of expressions is explicitly assigned to where to be used and does not overlap with each other. Thus, 'degree in A' is defined corresponding to the way to express terms in each context.

Example 4.1.3. For $p = 3$, using Maple[1] and writing terms as in (4.1.2), we have

- $\Lambda_0 A^2B^2 = 2A^2B + A^2$;
- $\Lambda_0^2 A^2B^2 = 2A^2$;
- $\Lambda_1 A^2B^2 = 2AB^2 + B^2 + (\Omega_1^{-1} + 2d)A^2B + (2\Omega_1^{-1} + 2d)AB + (d\overline{\Omega} + \Omega_1^{-1})B + (d\Omega_1^{-1} + \Omega_1^{-2})A^2 + (d^2\overline{\Omega} + d\Omega_1^{-1} + 2\Omega_1^{-2} + 1)A + 2\overline{\Omega} + 2d\Omega_1^2\beta_1 + \Omega_1^{-2} + 1$;
- $\Lambda_1^2 A^2B^2 = 2B^2 + 2dA^2B + (\Omega_1^{-1} + d)AB + dB + (d\Omega_1^{-1} + 2\Omega_1^{-2})A^2 + (2\overline{\Omega} + 1)A + (\overline{\Omega} + d\Omega_1^2\beta_1 + d\Omega_1^{-1} + 2\Omega_1^{-2} + 1)$;
- $\Lambda_0\Lambda_1 A^2B^2 = AB + 2B + (\Omega_1^{-1} + 2d)A^2 + (2\Omega_1^{-1} + 2d + 2)A + d\overline{\Omega} + \Omega_1^{-1} + 1$;
- $\Lambda_0^2\Lambda_1 A^2B^2 = A + 2$;
- $\Lambda_0\Lambda_1^2 A^2B^2 = B + 2dA^2 + (\Omega_1^{-1} + d)A + d + 2$;
- $\Lambda_0^2\Lambda_1^2 A^2B^2 = 1$.

As the shape of Λ_1 is complicated, it is unsurprising that the formula we obtained is even more so. Besides, we have to confront more tortuous objects like $\Lambda_0^i\Lambda_1^j$ where $0 \leq i, j \leq p-1$. Without some techniques, it seems to be impossible to move forwards.

Let us record the summary table below containing all the algebraic and arithmetic information required in this study. Note that, with the unified language, all the algebraic actions are given by the same formulae in non-classical Hopf-Galois structures. Unfortunately, this is not the case for the arithmetic considerations involving valuations and this leads to different results in the two types of all the non-classical Hopf-Galois structures. Nevertheless, this allows us to successfully construct a scaffold.

[1]mathematical software

	Non-special	Special
Algebraic	$A^p - A = \overline{\Omega}$ $\tau(A) = A$ $\tau(B) = B + 1$ $\sigma(A) = A + 1$ $\sigma(B) = B - \Omega_1^{-1}$	$A^p - A = \overline{\Omega}$ $\tau(A) = A$ $\tau(B) = B + 1$ $\sigma(A) = A + 1$ $\sigma(B) = B - \Omega_1^{-1}$
Arithmetic	$v_L(A) = -p^2w - pb$ $v_L(B) = -b$ $v_L(\Omega_1) = -p^2w$ $v_L(\beta_1) = -p^2b$ $v_L\left(\overline{\Omega}\right) = -p^3w - p^2b$	$v_L(A) = -pb$ $v_L(B) = -p^2w - b$ $v_L(\Omega_1) = p^2w$ $v_L(\beta_1) = -p^3w - p^2b$ $v_L\left(\overline{\Omega}\right) = -p^2b$

Table 3: Summary table of algebraic and arithmetic actions in various Hopf-Galois structures on a near one-dimensional elementary abelian extension.

4.2 Ordering Terms in L

Before we move on, it is worth mentioning that all the algebraic results onwards can be translated from unified language to every non-classical Hopf-Galois structure on L/K since every single move from now on is based on nothing else but what is stated in Table 3 (algebraic part).

Definition 4.2.1. Writing in terms of the basis A^iB^j for $0 \leq i, j \leq p-1$, we say A^iB^j is *colexicographically higher* than $A^{i'}B^{j'}$ and denote by $A^iB^j \succ A^{i'}B^{j'}$ if $j > j'$ or if $j = j'$ then $i > i'$. In this ordering, we ignore coefficients in K. Also, we make the convention that 0 is the least colexicographical order followed by 1.

For example, we have that $AB^2 \succ A^{p-1}B$. However, $A^pB^2 \not\succ A^2B^2$. This is because under the basis A^iB^j for $0 \leq i, j \leq p-1$, we have that $A^pB^2 = AB^2 + \overline{\Omega}B^2$ and $A^2B^2 \succ AB^2$, $A^2B^2 \succ \overline{\Omega}B^2$. The latter example emphasises on the necessity of how to write expressions in L in the context of colexicographical order.

The importance of the colexicographical order will be mainly seen in the next chapter as a systematic way for the elimination process. Also, in this chapter, it

can be used to simplify some complicated expressions arising from actions of Λ_0 and Λ_1, which is Lemma 4.2.5. In particular, this lemma is the main ingredient for the elimination process of the construction of Φ in Lemma 5.1.3.

Proposition 4.2.2. *The colexicographically highest term in* $\Lambda_1 A^r B^s$ *is*

$$\begin{cases} rA^{r-1}B^s & \text{if } r \geq 1 \\ -dsAB^{s-1} & \text{if } r = 0, s \neq 0 \\ 0 & \text{if } r = 0, s = 0. \end{cases}$$

Proof. From (4.1.2) in Proposition 4.1.2, if $r \geq 1$, the degree of B is the highest when $u = 0$ and then v must be $r - 1$. Note that it is not necessary to consider the second and third summation since $u = 0$. Also, the fourth one can be ignored because even if $s = p-1$ the first summation gives higher terms. If $r = 0$, we only have the terms from the first summation. The highest term is from when $u = 1$ and $v = 0$. □

Remark.

(*i*) Λ_1 always reduces colexicographical order.

(*ii*) It is clear from Proposition 4.1.2(i) that if $s \neq 0$, then Λ_0 respects colexicographical order. That is, if $s \neq 0$ and $A^r B^s \succ A^{r'} B^{s'}$, then $\Lambda_0 A^r B^s \succ \Lambda_0 A^{r'} B^{s'}$.

(*iii*) When $s = 0$, it follows from Proposition 4.2.2 that Λ_1 respects the colexicographical order; whereas it is not always the case if $s \neq 0$. In more detail, the only condition when Λ_1 fails to respect colexicographical order is $s \neq 0, r = 0, s-1 = s'$ and $r' \geq 2$. To see this, if $r \neq 0$, we have that Λ_1 respects the order since we have both $A^{r-1}B^s \succ A^{r'-1}B^{s'}$ and $A^{r-1}B^s \succ AB^{s'-1}$. Now, we suppose that $r = 0$. Then $s > s'$. If $s - 1 > s'$, we again have that Λ_1 respects the order because $AB^{s-1} \succ A^{r'-1}B^{s'}, AB^{s'-1}$. However, if $s - 1 = s'$, the only condition for $AB^{s-1} \succ A^{r'-1}B^{s'} = A^{r'-1}B^{s-1}$ is $r' < 2$. For instance, without caring about the coefficients in K, AB^{s-1} is the colexicographically highest term in both $\Lambda_1 B^s$ and $\Lambda_1 A^2 B^{s-1}$ although $B^s \succ A^2 B^{s-1}$.

For convenience, we define

Definition 4.2.3. Let $X, Y \in L$. Writing X, Y in terms of the basis $A^i B^j$ where $0 \leq i, j \leq p-1$, we write

$$X = Y + \mathcal{C}(A^r B^s)$$

if the colexicographically highest term in $X - Y$ has colexicographical order lower than $A^r B^s$.

For instance, from Example 4.1.3, we can write

$$\begin{aligned} \Lambda_0 A^2 B^2 &= 2A^2 B + \mathcal{C}(A^2 B), \\ \Lambda_0 A^2 B^2 &= 2A^2 B + \mathcal{C}(B), \\ \text{but} \quad \Lambda_0 A^2 B^2 &\neq 2A^2 B + \mathcal{C}(A^2). \end{aligned}$$

The new notation $\mathcal{C}$ allows us to simplify calculation by absorbing all the irrelevant terms.

Proposition 4.2.4. *Let $r \geq 1$ and let $X \in L$. If $X = kA^r B^s + \mathcal{C}(A^r B^s)$ for some $k \in K$, then $\Lambda_1 X = krA^{r-1} B^s + \mathcal{C}(A^{r-1} B^s)$.*

Proof. Assume that $X - kA^r B^s = \sum_{i=1}^{r} c_i A^{r-i} B^s + \sum_{j=1}^{s} \sum_{h=0}^{p-1} c_{h,j} A^h B^{s-j}$ for some $c_i, c_{h,j} \in K$. Then,

$$\Lambda_1 X - \Lambda_1 k A^r B^s = \Lambda_1 \left(\sum_{i=1}^{r} c_i A^{r-i} B^s + \sum_{j=1}^{s} \sum_{h=0}^{p-1} c_{h,j} A^h B^{s-j} \right).$$

From Proposition 4.2.2, the colexicographically highest term on the RHS is lower than $A^{r-1} B^s$. On the LHS, since $r \geq 1$, from the same proposition, the colexicographically highest term in $\Lambda_1 k A^r B^s$ is $rkA^{r-1} B^s$. Therefore,

$$\Lambda_1 X = krA^{r-1} B^s + \mathcal{C}(A^{r-1} B^s).$$

□

Lemma 4.2.5. *If $s \geq i$ and $r \geq j$, then the colexicographically highest term in $\Lambda_0^i \Lambda_1^j A^r B^s$ is*

$$i!j!\binom{s}{i}\binom{r}{j}A^{r-j}B^{s-i}.$$

Thus, we can simply write

$$\Lambda_0^i \Lambda_1^j A^r B^s = i!j!\binom{s}{i}\binom{r}{j}A^{r-j}B^{s-i} + \mathcal{C}(A^{r-j}B^{s-i}).$$

In particular, the colexicographically highest term in $\Lambda_0^i \Lambda_1^j A^{p-1} B^{p-1}$ is

$$(-1)^{i+j} i!j! A^{p-j-1} B^{p-i-1}.$$

Proof. First, computing the iteration of Λ_0 by Proposition 4.1.2(i), we have

$$\Lambda_0^i \Lambda_1^j A^r B^s = \Lambda_1^j \left[i!\binom{s}{i} A^r B^{s-i} + \mathcal{C}(A^r B^{s-i}) \right].$$

Then by Proposition 4.2.4 we have

$$\begin{aligned}
\Lambda_0^i \Lambda_1^j A^r B^s &= \Lambda_1^{j-1} \left[i!\binom{s}{i} r A^{r-1} B^{s-i} + \mathcal{C}(A^{r-1} B^{s-i}) \right] \\
&= \Lambda_1^{j-2} \left[i!\binom{s}{i} r(r-1) A^{r-2} B^{s-i} + \mathcal{C}(A^{r-2} B^{s-i}) \right] \\
&\vdots \\
&= i!\binom{s}{i} r(r-1)(r-j+1) A^{r-j} B^{s-i} + \mathcal{C}(A^{r-j} B^{s-i}) \\
&= i!j!\binom{s}{i}\binom{r}{j} A^{r-j} B^{s-i} + \mathcal{C}(A^{r-j} B^{s-i}).
\end{aligned}$$

In particular, when $r = s = p - 1$, we have

$$i!j!\binom{p-1}{i}\binom{p-1}{j} = (-1)^{i+j} i!j!.$$

□

Then, we provide an immediate consequence of Lemma 4.2.5.

Corollary 4.2.6. *The term $A^{p-1}B^{p-1}$ is a normal basis generator for the Hopf-Galois structure $L[N_{T,d}]^G$.*

Remark. Corollary 4.2.6 asserts that $\Lambda_0^i\Lambda_1^j A^{p-1}B^{p-1}$ behaves algebraically well. Unfortunately, this is not the case for the arithmetic view since occasionally Λ_1 decreases the valuation dramatically by increasing the degree in A. This would be a sign that scaffolds might not exist as colexicographically highest terms occasionally fail to determine the valuation.

We end this section by considering things arithmetically. Noticing that, in Hopf-Galois structures arising from non-special subgroups, $v_L(A) \leq pv_L(B)$, we see degree of A is the first matter for determining the valuation. Although this is not the case in Hopf-Galois structures arising from the special subgroup, knowing the highest degree of A still allows us to very nearly complete the study. Recall that, from the proposition below to the next subsection, we write $\Lambda_0^i\Lambda_1^j A^r B^s$ in terms of $A^f B^g$ for $f, r \geq 0$ and $0 \leq g, s \leq p-1$. Here, f and r are allowed to be greater than p.

Proposition 4.2.7. *The maximal degree of A in $\Lambda_1^j A^r B^s$ with $p-1 \geq j \geq 1$ is at most*

$$\begin{cases} r+s & \text{if } j \leq s \\ r+2s-j & \text{if } j \geq s, r+2s-j \geq 0 \\ r-j & \text{if } j \leq r, s=0 \\ 0 & \text{if } j > r, s=0 \text{ or } j \geq s, s \neq 0, r+2s-j < 0. \end{cases}$$

Proof. Recall the formula (4.1.1)

$$\Lambda_1 A^r B^s = \sum_{u=0}^{s}\sum_{t=0}^{r}\binom{s}{u}\binom{r}{t}(-d)^u A^{r-t+u}(B-\Omega_1^{-1})^{s-u} + \sum_{v=0}^{r}\binom{r}{v}\delta_{s,p-1}A^v - A^r B^s.$$

If $s = 0$, it becomes just

$$\Lambda_1 A^r = \sum_{t=0}^{r} \binom{r}{t} A^{r-t} - A^r. \tag{4.2.1}$$

From (4.2.1), it is easy to see the two cases when $j \leq r, s = 0$ and $j > r, s = 0$.

Then, we observe the mechanism of action of Λ_1 on $A^r B^s$.

(1) Due to (4.1.1), Λ_1 can transfer degree from B to A.

(2) Λ_1 cannot increase degree of B.

(3) Without B, Λ_1 must decrease degree of A as in (4.2.1).

Hence, to attain degree of A as high as possible, we have to avoid (3) by letting Λ_1 gradually transfer degree from B to A. Once we have run out of B and Λ_1's still exist, let the remaining Λ_1's decrease degree of A.

Case $j \leq s$. By (1), $\Lambda_1^{j-1} A^r B^s$ contains the term $cA^{r+j-1}B^{s-j+1}$ for some $c \in K$. Note that c could be 0 but let us assume that it is not as we want to know the least upper bound of degree of A in $\Lambda_1^j A^r B^s$ when j, r, s are arbitrary. Then, again by (1), the maximal degree of A in $\Lambda_1^j A^r B^s = \Lambda_1 \Lambda_1^{j-1} A^r B^s$ is

$$(r + j - 1) + (s - j + 1) = r + s.$$

Case $j \geq s, r + 2s - j \geq 0$. By (1), $\Lambda_1^s A^r B^s$ contains the term cA^{r+s} for some $c \in K$. As in the previous case, we assume that $c \neq 0$. Then by (3), the maximal degree of A in $\Lambda_1^j A^r B^s = \Lambda_1^{j-s} \Lambda_1^s A^r B^s$ is $(r + s) - (j - s) = r + 2s - j$.

Case $j \geq s, r + 2s - j < 0$. We consider

$$\Lambda_1^j A^r B^s = \Lambda_1^{j-r-2s} \left(\Lambda_1^{r+2s} A^r B^s \right) = \Lambda_1^{j-r-2s} \left(\Lambda_1^{r+s} \Lambda_1^s A^r B^s \right).$$

As shown in the previous case, we know that the maximal degree of A and B in $\Lambda_1^{r+2s} A^r B^s$ are 0. In more detail, B^s transfers all its degree to A^r by Λ_1^s and then Λ_1^{r+s} decreases all the degree of A in A^{r+s}. Indeed, since $j - r - 2s > 0$, we have $\Lambda_1^j A^r B^s = \Lambda_1^{j-r-2s} \left(\Lambda_1^{r+2s} A^r B^s \right) = 0$. □

Remark. The proposition tells only the least upper bound of degree of A not the term with highest degree of A occurring in $\Lambda_1^j A^r B^s$. This is because the coefficient of the term whose degree of A is equal to the amount stated in the proposition might vanish (see Example 4.3.4 below). Yet, this proposition can allow us to simplify some complicated proofs later.

4.3 Computing Some Terms in $\Lambda_1^j A^r B^s$

In the next chapter, we have to face $\Lambda_1^j A^r B^s$. It is very exhausting or perhaps impossible to compute $\Lambda_1^j A^r B^s$ especially when p is large. Fortunately, we do not have to know every term in $\Lambda_1^j A^r B^s$ but only certain significant terms. The method enabling us to find them is called $(+,-)$-diagram.

4.3.1 Computing the coefficient of A^{r+2s-j} in $\Lambda_1^j A^r B^s$

Throughout this subsection, we fix j, r, s where $j \geq s \geq 1$ and $r + 2s - j \geq 1$. We aim to compute the term A^{r+2s-j} in $\Lambda_1^j A^r B^s$. Recall that $r+2s-j$ is the maximal degree of A in $\Lambda_1^j A^r B^s$ by Proposition 4.2.7. In the calculation, there are many terms coming out. However, there are only a few terms which can contribute A^{r+2s-j} at the end. To know the coefficient of A^{r+2s-j} in $\Lambda_1^j A^r B^s$, we provide an algorithm to construct a $(+,-)$-diagram after stating Lemma 4.3.2 and 4.3.3, which are the main ingredients of the algorithm.

Proposition 4.2.7 plays a major role in computing the coefficient. For convenience, we pick only the two cases required in this study as shown below. The maximal degree of A in $\Lambda_1^j A^f B^g$ is at most

$$\begin{cases} f + 2g - j & \text{if } j \geq g \quad \text{[Case 4.3.1]} \\ f + g & \text{if } j \leq g \quad \text{[Case 4.3.2].} \end{cases}$$

Also, we define:

Definition 4.3.1. Let $X, Y \in L$. We write

$$X = Y + \mathcal{T}^z$$

for some $z \in \mathbb{N}$ if $X - Y$ contains only terms, say $A^f B^g$, with the property that $f + 2g < z$.

With the notation $\mathcal{T}^z$, the formula (4.1.1) can be simply written as in the lemma below.

Lemma 4.3.2. *We have*

$$\Lambda_1 A^f B^g = \begin{cases} fA^{f-1}B^g - gdA^{f+1}B^{g-1} + \mathcal{T}^{f+2g-1} & \text{if } f \geq 1, g \geq 1 \\ -gdA^{f+1}B^{g-1} + \mathcal{T}^{f+2g-1} & \text{if } f = 0, g \geq 1 \\ fA^{f-1} + \mathcal{T}^{f-1} & \text{if } f \geq 1, g = 0. \end{cases}$$

Proof. Assume that $g \geq 1$. From the formula (4.1.1), if t is fixed, we observe that the maximal total degree is $f + g - t$. Hence, the sum of total degree and degree of B is at most

$$(f + g - t) + (g - u) = f + 2g - (t + u).$$

Consequently, those terms not absorbed in $\mathcal{T}^{f+2g-1}$ are colexicographically highest terms obtained from putting u, t such that

$$f + 2g - (t + u) \geq f + 2g - 1, \text{which is simplified to } u + t \leq 1.$$

For $u = 0, t = 1$, we obtain the term $fA^{f-1}B^g$ and for $u = 1, t = 0$, we obtain $-gdA^{f+1}B^{g-1}$. Note that if $f = 0$, we have only the latter term.

If $g = 0$, the lemma follows from (4.2.1) in the proof of Proposition 4.2.7. □

To compute the coefficient of A^{r+2s-j} in $\Lambda_1^j A^r B^s$, we have to act Λ_1 on $A^r B^s$ repeatedly j times. Hence, there are j steps in the algorithm for computing the

coefficient, which is clearly explained below. The principle of the algorithm is that in each step we know potential candidates which might contribute A^{r+2s-j} at the end by Lemma 4.3.2 and then decide which ones of them can do so by using [Case 4.3.1] or [Case 4.3.2]. The qualified terms are called 'contributors' as they can contribute A^{r+2s-j} at the end.

Algorithm for computing A^{r+2s-j} in $\Lambda_1^j A^r B^s$

Step 0: The contributor in this step is $A^r B^s$.

Step k $(1 \leq k \leq j-1)$***:*** Act Λ_1 on each contributor from the previous step, say $cA^f B^g$ for some $c \in \mathbb{F}_p$. Then, by Lemma 4.3.2, we know candidates for being contributors containing in $\Lambda_1 cA^f B^g$, which are

$$cfA^{f-1}B^g, \ -cgdA^{f+1}B^{g-1}, \ c\mathcal{T}^{f+2g-1}.$$

Next, compute the maximal degree of A in

$$\Lambda_1^{j-k} cfA^{f-1}B^g, \ \Lambda_1^{j-k}\left(-cgdA^{f+1}B^{g-1}\right), \ \Lambda_1^{j-k} c\mathcal{T}^{f+2g-1}$$

by [Case 4.3.1] or [Case 4.3.2]. Lastly, pass contributors happening in this step to the next step (i.e. terms which can give the maximal degree of A in the amount of $r+2s-j$).

Step j: We obtain the coefficient of A^{r+2s-j}, which is the sum of the coefficients of the contributors happening in step $j-1$.

To simplify the process of the determination of candidates, we present the lemma below.

Lemma 4.3.3. *Suppose that we are in step k and $A^f B^g$ is a contributor from the previous step. Then, considering terms on the RHS of Lemma 4.3.2, we have*

(i) $-gdA^{f+1}B^{g-1}$ is a contributor;

(ii) $\mathcal{T}^{f+2g-1}$ absorbs only terms failing to be contributors;

(iii) $fA^{f-1}B^g$ *can be a contributor iff* $f+g > r+2s-j$;

(iv) fA^{f-1} *is a contributor (if* $g=0$*);*

(v) $\mathcal{T}^{f-1}$ *absorbs only terms failing to be contributors (if* $g=0$*).*

Proof. We omit writing coefficients in K. We aim to decide which of the following terms can be contributors:

$$A^{f+1}B^{g-1},\ A^{f-1}B^g,\ \mathcal{T}^{f+2g-1},\ A^{f-1},\ \mathcal{T}^{f-1}.$$

This can be done by computing the maximal degree of A in

$$\Lambda_1^{j-k}A^{f+1}B^{g-1},\ \Lambda_1^{j-k}A^{f-1}B^g,\ \Lambda_1^{j-k}\mathcal{T}^{f+2g-1},\ \Lambda_1^{j-k}A^{f-1},\ \Lambda_1^{j-k}\mathcal{T}^{f-1}$$

by employing [Case 4.3.1] or [Case 4.3.2]. Only terms with the highest amount of degree of A will become contributors.

(i)-(iii) Considering $A^{f+1}B^{g-1},\ A^{f-1}B^g,\ \mathcal{T}^{f+2g-1}$, we know that at least one of them must be a contributor since otherwise we do not have terms contributing A^{r+2s-j} at the end. To determine which terms can be, we first prove the claim below. Note that the claim allows us to know which of [Case 4.3.1] and [Case 4.3.2] we have to employ.

Claim: *If we are in step* k *and* A^fB^g *is a contributor from the previous step, then* $j-k \geq g-1$.

We prove by induction on step number k. Obviously, the claim holds when $k=1$ since A^rB^s is a contributor from the previous step (step 0) and $j-1 \geq s-1$. Recall that $j \geq s$.

Now, suppose that the claim holds in step k and A^fB^g is a contributor from the previous step with the property that $j-k \geq g-1$. By Lemma 4.3.2, we know

that

$$A^{f+1}B^{g-1},\ A^{f-1}B^{g},\ \mathcal{T}^{f+2g-1}$$

are candidates for being contributors in step k. To decide which terms can be contributors and sent to step $k+1$, we compute the maximal degree of A in

$$\Lambda_1^{j-k}A^{f+1}B^{g-1},\ \Lambda_1^{j-k}A^{f-1}B^{g},\ \Lambda_1^{j-k}\mathcal{T}^{f+2g-1}.$$

- The maximal degree of A in $\Lambda_1^{j-k}A^{f+1}B^{g-1}$ is at most

$$\begin{cases} f+2g-1-j+k & \text{if } j-k \geq g \qquad \text{(by [Case 4.3.1])}; \\ f+g & \text{if } j-k=g-1 \quad \text{(by [Case 4.3.2])}. \end{cases}$$

- The maximal degree of A in $\Lambda_1^{j-k}A^{f-1}B^{g}$ is at most

$$\begin{cases} f+2g-1-j+k & \text{if } j-k \geq g \qquad \text{(by [Case 4.3.1])}; \\ f+g-1 & \text{if } j-k=g-1 \quad \text{(by [Case 4.3.2])}. \end{cases}$$

In terms of $\mathcal{T}^{f+2g-1}$, we assume that A^xB^y is contained in $\mathcal{T}^{f+2g-1}$. Then, we have $y \leq g$ and $x+2y < f+2g-1$ (by definition of $\mathcal{T}$). The maximal degree of A in $\Lambda_1^{j-k}A^xb^y$ is at most

$$\begin{cases} x+2y-j+k < f+2g-1-j+k & \text{if } j-k \geq g; \\ x+y < f+g-1 < f+g & \text{if } j-k=g-1 \text{ and } y=g; \\ x+2y-j+k < f+2g-1-j+k = f+g & \text{if } j-k=g-1 \text{ and } y \leq g-1. \end{cases}$$

If $j-k \geq g$, the contributors sent to step $k+1$ are both $A^{f+1}B^{g-1}$ and $A^{f-1}B^{g}$ since their amount of maximal degree of A is highest. This implies that the claim holds in step $k+1$ in this case as $j-(k+1) \geq (g-1)-1$ and $j-(k+1) \geq g-1$.

On the other hand, if $j-k=g-1$, we have the only one contributor sent to step $k+1$, which is $A^{f+1}B^{g-1}$. The claim still holds in this cases since $j-(k+1) \geq$

$(g-1)-1$. Therefore, the claim is proved.

Moreover, since $j-k \geq g$, we learn from the proof of the claim that $A^{f+1}B^{g-1}$ is always a contributor and hence

$$r+2s-j = f+2g-1-j+k;$$

whereas all the terms absorbed in $\mathcal{T}^{f+2g-1}$ fail to be. In terms of $A^{f-1}B^g$, we see that it can be a contributor iff $j-k \geq g$. This is equivalent to $f+g > r+2s-j$ as $r+2s-j = f+2g-1-j+k$.

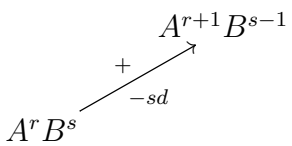
(iv) and (v) Suppose we are in step k. From the last case of Lemma 4.3.2, A^{f-1} is a contributor as long as A^f is a contributor in step $k-1$. This means the maximal degree of A in $\Lambda_1^{j-(k-1)}A^f$ is at most $f-j+k-1 = r+2s-j$. Thus, the maximal degree of A in $\Lambda_1^{j-k}A^{f-1}$ is at most $f-1-j+k = r+2s-j$. Note that all the terms absorbed in $\mathcal{T}^{f-1}$, which are only of the type A^t for some $t \lneq f-1$, fail to be contributors. □

Having Lemma 4.3.3, we can provide the algorithm along with how to construct a $(+,-)$-diagram to compute the coefficient of A^{r+2s-j} in $\Lambda_1^j A^r B^s$. Recall that $j \geq s \geq 1$ and $r+2s-j \geq 1$.

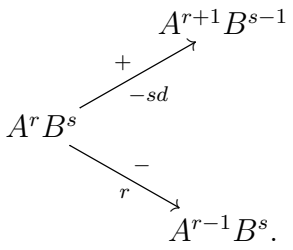
Step 1:

$$A^rB^s \text{ originates } \begin{cases} -sdA^{r+1}B^{s-1} & \text{as a contributor and} \\ rA^{r-1}B^s & \text{as a contributor if } r \neq 0, j-s \neq 0. \end{cases}$$

If $j = s$ or $j > s, r = 0$, we draw a diagram.



If $j > s$ and $r \geq 1$, we do



For more explanation of the diagrams, we draw

$$A^r B^s \xrightarrow[-sd]{+} A^{r+1}B^{s-1}$$

to mean that $-sdA^{r+1}B^{s-1}$ is a contributor contained in $\Lambda_1 A^r B^s$. The sign '+' indicates that the degree of A of the contributor is increased by 1 from the original term at the expense of degree of B. We draw

$$A^r B^s \xrightarrow[r]{-} A^{r-1}B^s$$

to mean that $rA^{r-1}B^s$ is a contributor contained in $\Lambda_1 A^r B^s$. The sign '$-$' indicates that the degree of A of this contributor is decreased by 1 from the original term; whereas the degree of B stays the same. Each number under each arrow is called a *transition coefficient*.

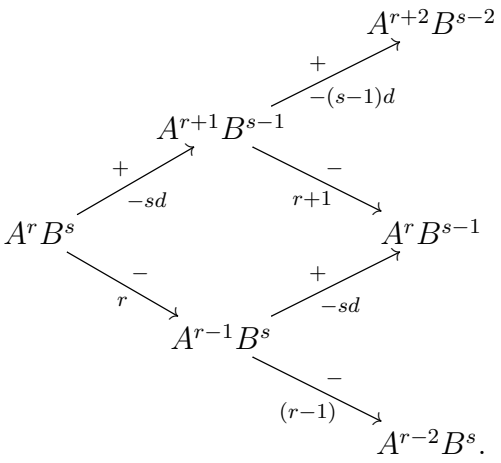
Step i $(1 < i \leq j)$***:*** Each contributor from the previous step, say $A^f B^g$, has to go with

$$\begin{cases} + & \text{if } g \neq 0 \text{ by Lemma 4.3.3(i);} \\ - & \text{if } f + g > r + 2s - j \text{ and } f \neq 0 \text{ by Lemma 4.3.3(iii) or (iv).} \end{cases}$$

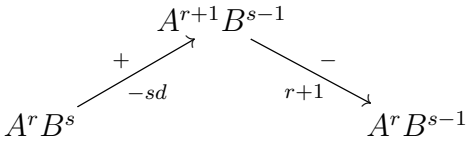
The algorithm terminates once A^{r+2s-j} appears.

After knowing contributors in each step, we draw an extension diagram on the diagram in the previous step. For example, if we are in step 2 and assume further that we receive two contributors from step 1 and each contributor in step 1 can

originate two contributors in step 2, then we draw the diagram



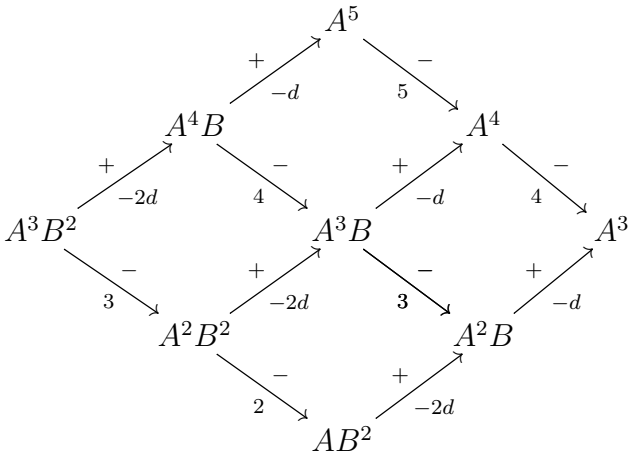
The diagram allows us to compute contributors happening in each step easily. For instance, the path



means that $-(r+1)sdA^rB^{s-1}$ is a contributor contained in $\Lambda_1^2 A^r B^s$. Note that the coefficient of A^rB^{s-1} from this path is obtained from the product of the transition coefficients. Also, the degree of Λ_1 is equal to the number of arrows.

Remark. While a $(+,-)$-diagram is running, it is possible that a transition coefficient might be equal to p in some paths. If this happens, we can still carry on performing. But note that the product of all the transition coefficients of these paths will vanish. See e.g. the example below.

Example 4.3.4. For $p = 5$, the $(+,-)$-diagram for computing the coefficient of A^3 in $\Lambda_1^4 A^3 B^2$ is shown below. Note that, in this case, we have $r = 3,\ s = 2$ and $j = 4$. Then, by Proposition 4.2.7, the maximal degree of A is at most 3.



Therefore, the coefficient of A^3 in $\Lambda_1^4 A^3B^2$ is 0 since

$$40d^2 + 32d^2 + 24d^2 + 12d^2 + 18d^2 + 24d^2 \equiv 0 \pmod 5.$$

With a $(+,-)$-diagram, we can compute some terms we need to know in the proof of Lemma 5.1.3.

Lemma 4.3.5. *(i) The coefficient of A^{p-3} in $\Lambda_1^{p-1}B^{p-2}$ is $-d^{p-2}$.*
(ii) The coefficient of A^{p-3} in $\Lambda_1^{p-3}B^{p-3}$ is $d^{p-3}(p-3)!$.

Proof. (i) The $(+,-)$-diagram for this problem is

$$\begin{array}{ccccccccc}
B^{p-2} & \xrightarrow[-(p-2)d]{+} & AB^{p-3} & \xrightarrow[-(p-3)d]{+} & A^2B^{p-4} & \xrightarrow[-(p-4)d]{+} & \cdots & \xrightarrow[-2d]{+} & A^{p-3}B \xrightarrow[-d]{+} A^{p-2} \\
 & & \Big\downarrow -1 & & \Big\downarrow -2 & & & & \Big\downarrow -p-3 \qquad \Big\downarrow -p-2 \\
 & & B^{p-3} & \xrightarrow[-(p-3)d]{+} & AB^{p-4} & \xrightarrow[-(p-4)d]{+} & \cdots & \xrightarrow[-2d]{+} & A^{p-4}B \xrightarrow[-d]{+} A^{p-3}.
\end{array}$$

There are $p-2$ terms of A^{p-3} with various coefficients happening from this action and the exact coefficient of A^{p-3} is

$$\begin{aligned}
(-d)^{p-2}\left[(p-2)! + 2(p-2)! + \ldots + (p-2)(p-2)!\right] &\equiv (-d)^{p-2}\left[1 + 2 + \ldots + (p-2)\right] \\
&\qquad \text{(by Wilson's theorem)} \\
&\equiv -d^{p-2} \pmod p.
\end{aligned}$$

(ii) We construct

$$B^{p-3} \xrightarrow[-(p-3)d]{+} AB^{p-4} \xrightarrow[-(p-4)d]{+} A^2B^{p-5} \xrightarrow[-(p-5)d]{+} \cdots \xrightarrow[-2d]{+} A^{p-4}B \xrightarrow[-d]{+} A^{p-3}.$$

Thus, $d^{p-3}(p-3)!$ is the coefficient of A^{p-3} in $\Lambda_1^{p-3}B^{p-3}$. □

4.3.2 Computing the coefficient of A^2B^{p-3} in $\Lambda_1^{p-1}A^{p-1}B^{p-2}$

We provide an algorithm for constructing the $(+,-)$-diagram for computing the coefficient of A^2B^{p-3} in $\Lambda_1^{p-1}A^{p-1}B^{p-2}$. As in subsection 4.3.1, we have Lemma 4.3.6 allowing us to know candidates for being contributors like Lemma 4.3.2 and Lemma 4.3.7 acting as Lemma 4.3.3 to decide which candidates are qualified to be contributors.

We come back to use the notation $\mathcal{C}$ (see Definition 4.2.3) to collect all the irrelevant terms in this subsection as the notation $\mathcal{T}$ does not really fit in this context.

Lemma 4.3.6. *For $1 \leq r \leq p-1$, we have*
(i)

$$\Lambda_1 A^r B^{p-2} = \begin{cases} -A^{p-2}B^{p-2} + \sum_{t=2}^{p-1}(-1)^t A^{p-1-t}B^{p-2} \\ \qquad + \mathcal{C}\left(B^{p-2}\right) & \text{if } r = p-1; \\ rA^{r-1}B^{p-2} + 2dA^{r+1}B^{p-3} + \sum_{t=2}^{r}\binom{r}{t}A^{r-t}B^{p-2} \\ \qquad + \mathcal{C}(A^{r+1}B^{p-3}) & \text{if } r < p-1. \end{cases}$$

(ii) $\Lambda_1 A^r B^{p-3} = rA^{r-1}B^{p-3} + \mathcal{C}(A^{r-1}B^{p-3})$.

Proof. (i) We observe that if $r = p-1$, (i) is obtained from collecting terms with colexicographical order at most B^{p-2} in (4.1.1); whereas from collecting terms with colexicographical order at most $A^{r+1}B^{p-3}$ if $r < p-1$. Although there are two cases for r, we can first consider r to be arbitrary as explained below. Note that,

from (4.1.1), it suffices to consider the cases $u = 0,\ 1 \leq t \leq r$ and $u = 1, t = 0$, since otherwise all terms will be absorbed in $\mathcal{C}\,(B^{p-2})$ or $\mathcal{C}(A^{r+1}B^{p-3})$.

- We have $rA^{r-1}B^{p-2}$ is the colexicographically highest term in

$$\binom{r}{1} A^{r-1}(B - \Omega_1^{-1})^{p-2} = rA^{r-1}(B - \Omega_1^{-1})^{p-2}$$

by putting $u = 0, t = 1$ in (4.1.1). The rest of terms i.e.

$$rA^{r-1}(B - \Omega_1^{-1})^{p-2} - rA^{r-1}B^{p-2}$$

will be absorbed in $\mathcal{C}$.

- For $r \geq t \geq 2$, we have $\binom{r}{t} A^{r-t}B^{p-2}$ is the colexicographically highest term in

$$\binom{r}{t} A^{r-t}(B - \Omega_1^{-1})^{p-2}$$

by putting $u = 0$ in (4.1.1). Similarly as above, we absorb

$$\binom{r}{t} A^{r-t}(B - \Omega_1^{-1})^{p-2} - \binom{r}{t} A^{r-t}B^{p-2}$$

in $\mathcal{C}$. Since $t = 2, \ldots, r$, we have $\displaystyle\sum_{t=2}^{r} \binom{r}{t} A^{r-t}B^{p-2}$ is a surviving term. This completes the proof when $r = p - 1$. If $r < p - 1$, we continue considering as below.

- We have $2dA^{r+1}B^{p-3}$ is the colexicographically highest term in

$$\binom{p-2}{1} (-d) A^{r+1}(B - \Omega_1^{-1})^{p-3}$$

by putting $u = 1, t = 0$ in (4.1.1). Absorbing

$$2dA^{r+1}(B - \Omega_1^{-1})^{p-3} - 2dA^{r+1}B^{p-3}$$

in $\mathcal{C}$, we are done.

(ii) Done by Lemma 4.2.5. □

Lemma 4.3.7. *Let $k \geq 1$. Then, $\Lambda_1^k A^r B^s$ does not contain A^2B^{p-3} if*

(i) $s = p-2,\ r < k$;

(ii) $s = p-3,\ 0 \leq r < k+2$; *or*

(iii) $s < p-3$.

Proof. (iii) The case $s < p-3$ is easy since Λ_1 cannot increase degree of B.

(i) For $s = p-2, r < k$, by Lemma 4.2.5, we have

$$\Lambda_1^k A^r B^{p-2} = \Lambda_1^{k-r}\Lambda_1^r A^r B^{p-2} = \Lambda_1^{k-r}\left(r!B^{p-2} + \mathcal{C}(B^{p-2})\right).$$

It is impossible for $\Lambda_1^{k-r}B^{p-2}$ to contain A^2B^{p-3} since from (4.1.1) we cannot have terms containing A^2 without sacrificing B^2.

To see that $\Lambda_1^{k-r}\mathcal{C}(B^{p-2})$ does not contain A^2B^{p-3}, we first find the (possibly) colexicographically highest term in $\Lambda_1^r A^r B^{p-2} - r!B^{p-2}$. To preserve the degree of B as high as possible, we can let only one Λ_1 decrease degree of B in A^rB^{p-2} (by transferring degree to A) and then Λ_1^{r-1} must decrease degree of A. This means that the (possibly) colexicographically highest term in $\Lambda_1^r A^r B^{p-2} - r!B^{p-2}$ is

$$A^{r+1-(r-1)}B^{(p-2)-1} = A^2B^{p-3}.$$

Since $k - r > 0$, it is impossible that $\Lambda_1^{k-r}\mathcal{C}(B^{p-2})$ can contain A^2B^{p-3}.

(ii) Obviously, $\Lambda_1^k A^r B^{p-3}$ does not contain A^2B^{p-3} if $r \leq 2$. So, we suppose that $3 \leq r < k+2$. Then, we have

$$\begin{aligned}
\Lambda_1^k A^r B^{p-3} &= \Lambda_1^{k-r+2}\Lambda_1^{r-2} A^r B^{p-3} \\
&= \Lambda_1^{k-r+2}\left((r-2)!\binom{r}{r-2}A^2B^{p-3} + \mathcal{C}(A^2B^{p-3})\right) \\
&= \Lambda_1^{k-r+2}\left(\frac{r!}{2}A^2B^{p-3} + \mathcal{C}(A^2B^{p-3})\right).
\end{aligned}$$

Since $k - r + 2 \geq 1$, the colexicographically highest term in

$$\Lambda_1^{k-r+2}\left(\frac{r!}{2}A^2B^{p-3} + \mathcal{C}(A^2B^{p-3})\right)$$

must be lower than A^2B^{p-3}. □

Now, we are ready to explain the algorithm. Note that each step refers to each number of Λ_1 acting on $A^{p-1}B^{p-2}$.

Step 1: By Lemma 4.3.6(i) case $r = p - 1$, we have

$$\Lambda_1 A^{p-1}B^{p-2} = -A^{p-2}B^{p-2} + \sum_{t=2}^{p-1}(-1)^t A^{p-1-t}B^{p-2} + \mathcal{C}\left(B^{p-2}\right).$$

Next, by Lemma 4.3.7 with putting $k = p - 2$, the only one surviving term is

$$(p-1)A^{p-2}B^{p-2}.$$

Like in subsection 4.3.1, any term not filtered out by Lemma 4.3.7 is called a *contributor*. It might not be foreseeable that contributors in most steps (especially in early ones) can truly contribute A^2B^{p-3} at the end. However, we will see later that only those terms satisfying the condition for being contributors above can truly do so. Then, we draw the $(+,-)$-diagram for this first step as

$$A^{p-1}B^{p-2} \xrightarrow[p-1]{-} A^{p-2}B^{p-2}.$$

Step 2: Apply Λ_1 on $(p-1)A^{p-2}B^{p-2}$. By Lemma 4.3.6(i), we know candidates for being contributors in this step. Then, taking $k = p - 3$ in Lemma 4.3.7 gives the contributors which are

$$(p-1)(p-2)A^{p-3}B^{p-2} \text{ and } -(p-1)(p-2)dA^{p-1}B^{p-3}.$$

The $(+,-)$-diagram is drawn as

$$\begin{array}{ccccc} & & A^{p-1}B^{p-3} & & \\ & & \Big\uparrow{\scriptstyle +} \quad {\scriptstyle -(p-2)d} & & \\ A^{p-1}B^{p-2} & \xrightarrow[p-1]{-} & A^{p-2}B^{p-2} & \xrightarrow[p-2]{-} & A^{p-3}B^{p-2}. \end{array}$$

To set the inductive step, we prove the claim:

CLAIM. *For $2 \leq i < p-1$, the contributors happening in step i are precisely*

$$c_1^{(i-1)}(p-i)A^{p-i-1}B^{p-2} \text{ and } \left[-c_1^{(i-1)}(p-2)d + c_2^{(i-1)}(p-i+2)\right] A^{p-i+1}B^{p-3}$$

where $c_1^{(i-1)}, c_2^{(i-1)}$ are defined recursively as

$$c_1^{(i)} = c_1^{(i-1)}(p-i) \text{ and } c_2^{(i)} = -c_1^{(i-1)}(p-2)d + c_2^{(i-1)}(p-i+2)$$

with the initial conditions $c_1^{(1)} = p-1$ and $c_2^{(1)} = 0$.

Proof. For $i = 2$, we see from step 1 that $c_1^{(1)} = p-1$ and $c_2^{(1)} = 0$. Moreover, step 2 above confirms that the claim holds for $i = 2$. Now, assume that the claim holds for $i \leq p-3$. Hence, in step $i+1$, the contributors received from step i are

$$c_1^{(i-1)}(p-i)A^{p-i-1}B^{p-2} \text{ and } \left[-c_1^{(i-1)}(p-2)d + c_2^{(i-1)}(p-i+2)\right] A^{p-i+1}B^{p-3}.$$

Since $c_1^{(i)} = c_1^{(i-1)}(p-i)$ and $c_2^{(i)} = -c_1^{(i-1)}(p-2)d + c_2^{(i-1)}(p-i+2)$, we have that the contributors above simply are

$$c_1^{(i)}A^{p-i-1}B^{p-2} \text{ and } c_2^{(i)}A^{p-i+1}B^{p-3}.$$

By Lemma 4.3.6, we have

$$\begin{aligned}\Lambda_1 A^{p-i-1}B^{p-2} = \ & (p-i-1)A^{p-i-2}B^{p-2} - (p-2)dA^{p-i}B^{p-3} \\ & + \sum_{t=2}^{p-i-1} \binom{p-i-1}{t} A^{p-i-t-1}B^{p-2} + \mathcal{C}\left(A^{p-i}B^{p-3}\right)\end{aligned}$$

and

$$\Lambda_1 A^{p-i+1}B^{p-3} = (p-i+1)A^{p-i}B^{p-3} + \mathcal{C}\left(A^{p-i}B^{p-3}\right).$$

Taking $k = p-i-2$ in Lemma 4.3.7, we have that the contributors in step $i+1$ are

$$c_1^{(i)}(p-i-1)A^{p-i-2}B^{p-2} \text{ and } \left[-c_1^{(i)}(p-2)d + c_2^{(i)}(p-i+1)\right] A^{p-i}B^{p-3}.$$

Thus, the claim holds in step $i+1$. □

Step i $(3 \leq i < p-1)$***:*** For convenience, let us ignore coefficients in $\mathbb{F}_p$. From the claim, we receive $A^{p-i}B^{p-2}$ and $A^{p-i+2}B^{p-3}$ from the previous step and we see that $A^{p-i}B^{p-2}$ must go with both $+$ and $-$ to obtain the contributors in step i which are $A^{p-i+1}B^{p-3}$ and $A^{p-i-1}B^{p-2}$ respectively. On the other hand, the contributor $A^{p-i+2}B^{p-3}$ from the previous step must go with $-$ only. This yields the other contributor $A^{p-i+1}B^{p-3}$ in step i.

Thus, in step $p-2$, the $(+,-)$-diagram is drawn as

$$\begin{array}{ccccccccc} & & A^{p-1}B^{p-3} & \xrightarrow[p-1]{-} & A^{p-2}B^{p-3} & \xrightarrow[p-2]{-} & \cdots & \xrightarrow[4]{-} & A^3B^{p-3} \\ & & {\scriptstyle +}\uparrow{\scriptstyle -(p-2)d} & & {\scriptstyle +}\uparrow{\scriptstyle -(p-2)d} & & & & {\scriptstyle +}\uparrow{\scriptstyle -(p-2)d} \\ A^{p-1}B^{p-2} & \xrightarrow[p-1]{-} & A^{p-2}B^{p-2} & \xrightarrow[p-2]{-} & A^{p-3}B^{p-2} & \xrightarrow[p-3]{-} & \cdots & \xrightarrow[3]{-} & A^2B^{p-2} \xrightarrow[2]{-} AB^{p-2} \end{array}$$

Step $p-1$***:*** From the diagram above, the contributors received from the step $p-2$

are AB^{p-2} and A^3B^{p-3}. By Lemma 4.3.6, we have

$$\begin{aligned}\Lambda_1 AB^{p-2} &= B^{p-2} - (p-2)dA^2B^{p-3} + \mathcal{C}\left(A^2B^{p-3}\right),\\ \Lambda_1 A^3B^{p-3} &= 3A^2B^{p-3} + \mathcal{C}\left(A^2B^{p-3}\right).\end{aligned}$$

Therefore, the final diagram is drawn as

$$\begin{array}{ccccccccc} & & A^{p-1}B^{p-3} & \xrightarrow[p-1]{-} & A^{p-2}B^{p-3} & \xrightarrow[p-2]{-} & \cdots & \xrightarrow[4]{-} & A^3B^{p-3} \xrightarrow[3]{-} A^2B^{p-3} \\ & & {\scriptstyle +}\uparrow{\scriptstyle -(p-2)d} & & {\scriptstyle +}\uparrow{\scriptstyle -(p-2)d} & & & & {\scriptstyle +}\uparrow{\scriptstyle -(p-2)d} \quad {\scriptstyle +}\uparrow{\scriptstyle -(p-2)d} \\ A^{p-1}B^{p-2} & \xrightarrow[p-1]{-} & A^{p-2}B^{p-2} & \xrightarrow[p-2]{-} & A^{p-3}B^{p-2} & \xrightarrow[p-3]{-} & \cdots & \xrightarrow[3]{-} & A^2B^{p-2} \xrightarrow[2]{-} AB^{p-2}. \end{array}$$

Lemma 4.3.8. *The coefficient of A^2B^{p-3} in $\Lambda_1^{p-1}A^{p-1}B^{p-2}$ is d.*

Proof. Due to the final diagram, we have the coefficient is

$$\begin{aligned}-(p-2)d(p-1)(p-2)\cdots 3\left((p-1)+(p-2)+\cdots+2\right) &= d(p-1)!(p-1)\\ &= d.\end{aligned}$$

□

Chapter 5

The Main Lemma

Due to the remark on Corollary 4.2.6, the possibility of having scaffolds is likely to be slim. We then provide the main lemma (Lemma 5.1.3), an essential key to show that, in most Hopf-Galois structures on L/K, no ideal of the valuation ring is free over its associated order.

5.1 Elimination Process

The idea to show the non-freeness of ideals over their associated orders is based on Theorem 5.1.1 and Lemma 5.1.2 published in [By97] by Byott.

Theorem 5.1.1. *Let $\mathfrak{P}_L^h$ be an ideal of $\mathfrak{O}_L$. If $\mathfrak{A} := \mathfrak{A}(h, L[N]^G)$ is a local ring and there exists a generating set $\{m_1, ..., m_n\}$ for $\mathfrak{P}_L^h$ over $\mathfrak{A}$ with the property that $\mathfrak{A}m_i \neq \mathfrak{P}_L^h$ for all i, then $\mathfrak{P}_L^h$ is not free as an $\mathfrak{A}$-module.*

Proof. See [By97, Theorem 2.1]. □

Note that we change notations in [By97] to the notations used in this thesis. Working over $\mathbb{F}_p$, we have that $\mathfrak{A}$ is local with the maximal ideal

$$\mathfrak{M} := \left\{ \sum_{i,j=0}^{p-1} a_{i,j} \Lambda_0^i \Lambda_1^j : a_{i,j} \in K, a_{0,0} \in \mathfrak{P}_K \right\} \cap \mathfrak{A}.$$

This is because the ideal $\mathfrak{M}$ contains non-units in $\mathfrak{A}$. Also, if $\alpha = \sum_{i,j=0}^{p-1} a_{i,j}\Lambda_0^i\Lambda_1^j \in \mathfrak{A} \setminus \mathfrak{M}$, then $a_{0,0} \in \mathfrak{O}_K \setminus \mathfrak{P}_K$. Then, we see that α is a unit in $\mathfrak{A}$ and its inverse in $\mathfrak{A}$ is $a_{0,0}^{-p}\alpha^{p-1}$.

A difficulty in employing Theorem 5.1.1 is to verify that $\mathfrak{A}m_i \neq \mathfrak{P}_L^h$, so Byott gave a criterion to check such a condition.

Lemma 5.1.2. *Let $m \in \mathfrak{P}_L^h$. If there exists $\alpha \in L[N]^G$ such that $\alpha m \in \mathfrak{P}_K\mathfrak{P}_L^h$ but $\alpha m' \notin \mathfrak{P}_K\mathfrak{P}_L^h$ for some $m' \in \mathfrak{P}_L^h$, then $\mathfrak{A}m \neq \mathfrak{P}_L^h$*

Proof. See [By97, Lemma 2.2]. □

To employ Lemma 5.1.2, we prove the lemma below.

Lemma 5.1.3 (**The main lemma**). *In any Hopf-Galois structure $L[N]^G$, there exists $\Phi \in L[N]^G$ satisfying the following properties:*

(i) $v_L\left(\left[\Lambda_1 + \Phi\right] A^{p-1}B^{p-1}\right) = v_L(A^{p-2}B^{p-1})$; *and*

(ii) $v_L\left(\left[\Lambda_1 + \Phi\right] B^{p-1}\right) \leq v_L(\overline{\Omega}A^{p-3})$.

According to the main lemma, we have to construct $\Phi \in L[N]^G$ such that $-A^{p-2}B^{p-1}$, the colexicographically highest term in $\Lambda_1 A^{p-1}B^{p-1}$, becomes the 'dominant term', the term of least valuation, in $[\Lambda_1 + \Phi]A^{p-1}B^{p-1}$. Also, our construction will enable us to give an upper bound on $v_L\left(\left[\Lambda_1 + \Phi\right] B^{p-1}\right)$. These two properties of Φ, together, will allow us to apply Lemma 5.1.2. The algorithm used to construct Φ is called the *Elimination process*.

The key idea of this process is to eliminate some terms especially ones with valuations less than $v_L(A^{p-2}B^{p-1})$ in descending colexicographical order by employing Lemma 4.2.5 along with choosing suitable coefficients in K. Bear in mind that every term must be written in terms of the basis A^iB^j with $0 \leq i, j \leq p-1$.

The question of comparing valuations of terms happening in the calculation is essential. From Table 3, in Hopf-Galois structures arising from non-special subgroups, we always have $v_L(A) < v_L(B)$. However, in Hopf-Galois structures

arising from the special subgroup, we cannot determine whether $v_L(A) < v_L(B)$ or $v_L(A) > v_L(B)$. This depends on the parameters b and w. This leads to a difficulty in performing the elimination process in every non-classical Hopf-Galois structure on L/K simultaneously.

In order to address this problem, we allow ourselves to use only common arithmetic properties holding in every non-classical Hopf-Galois structure and for every choice of b and w, i.e. $v_L(A),\ v_L(B),\ v_L(\Omega_1 B)$ and $v_L\left(\Omega_1^{-1}AB^{-1}\right)$ are negative, to decide which terms need to be eliminated.

For brevity, we define the notation $\mathcal{E}$ to absorb all the terms which need not to be eliminated.

Definition 5.1.4. In the unified language, we write

$$X = Y + \mathcal{E}$$

for $X, Y \in L$ if every term in $X - Y$ is colexicographically higher than AB^{p-3} and the condition that

$$v_L\left(A^{p-2}B^{p-1}\right) < v_L(X - Y)$$

is deducible only from the fact that, $v_L(A),\ v_L(B),\ v_L(\Omega_1 B)$ and $v_L\left(\Omega_1^{-1}AB^{-1}\right)$ are negative. In other words, we can obtain $v_L\left(A^{p-2}B^{p-1}\right) < v_L(X - Y)$ from the fact that $v_L(A),\ v_L(B),\ v_L(\Omega_1 B)$ and $v_L\left(\Omega_1^{-1}AB^{-1}\right)$ are negative.

Example 5.1.5. For $p \geq 5$, putting

$$X = \Omega_1^{-1}A^{p-1}B^{p-2} + \overline{\Omega}B^{p-2} + \Omega_1^{-2}A^{p-2}B^{p-3},$$

by the notation $\mathcal{E}$, we can write

$$X = \Omega_1^{-1}A^{p-1}B^{p-2} + \overline{\Omega}B^{p-2} + \mathcal{E}.$$

The term $\Omega_1^{-2}A^{p-2}B^{p-3}$ is absorbed in $\mathcal{E}$ because we have that the condition $v_L\left(A^{p-2}B^{p-1}\right) < v_L\left(\Omega_1^{-2}A^{p-2}B^{p-3}\right)$ is deducible from $v_L\left(\Omega_1^2 B^2\right) = 2v_L\left(\Omega_1 B\right) < 0$.

Also, note that $A^{p-1}B^{p-2}$, B^{p-2} and $A^{p-2}B^{p-3}$ are colexicographically higher than AB^{p-3}.

Then, the elimination process aims to eliminate terms in $\Lambda_1 A^{p-1}B^{p-1}$ with the following properties:

- they are not absorbed in $\mathcal{E}$; or
- their colexicographical order is lower than A^2B^{p-3}.

Note that the first property implies that all the terms, with colexicographical order higher than AB^{p-3} but valuation less than $v_L(A^{p-2}B^{p-1})$ in some non-classical Hopf-Galois structures on L/K or for some choices of b and w, need to be eliminated. Then, killing all the terms satisfying any of the properties above, we ensure that

$$v_L\left([\Lambda_1 + \Phi] \cdot A^{p-1}B^{p-1}\right) = v_L(A^{p-2}B^{p-1})$$

in every non-classical Hopf-Galois structure on L/K and for every choice of b and w. Although each step of the elimination process may introduce new terms with low valuation, this does not pose any problem since these new terms are colexicographically lower than the one being eliminated in that step. Thus, finally, they will be eliminated in some future steps.

Let us first perform the elimination process for $p \geq 5$.

Step 1: *Know terms in* $\Lambda_1 A^{p-1}B^{p-1}$.

Putting $r = s = p-1$ in Proposition 4.1.2(ii), we first roughly list the terms whose colexicographical order is at most A^2B^{p-3} :

- $A^{p-2-k}B^{p-1}$ for $0 \leq k \leq p-2$,
- $A^{p-1-k}B^{p-2}$ for $0 \leq k \leq p-1$,
- $A^{p-1-k}B^{p-3}$ for $0 \leq k \leq p-3$.

Next, we find the coefficients of these terms.

Coefficient of $A^{p-2}B^{p-1}$.

Applying Lemma 4.2.5, we have the coefficient is -1.

From now on, we consider each summation in (4.1.2) of Proposition 4.1.2(ii) with $r = s = p - 1$. Note that the fourth summation can be ignored.

Coefficient of $A^{p-3-k}B^{p-1}$ *for* $0 \leq k \leq p-3$.

- 1^{st} summation: Clearly, for each k, the pair (u, v) is $(0, p-3-k)$.
- 2^{nd} and 3^{rd} summation: We first observe that u must be 0. However, there is no v due to the condition $u + v \geq p$.

Thus, the coefficient of $A^{p-3-k}B^{p-1}$ for $0 \leq k \leq p-3$ is $(-1)^{p-3-k} = (-1)^k$.

Coefficient of $A^{p-1-k}B^{p-2}$ *for* $0 \leq k \leq p-1$.

Note that previously u could be only 0; however, in this situation, u can be either 0 or 1.

- 1^{st} summation: If $u = 0$, we have $v = p - 1 - k$ for all $k = 0, \ldots, p-1$. However, if $u = 1$, we see that $v = p-2-k$ only for $k = 0, \ldots, p-2$. Hence, this summation gives $(-1)^k(\Omega_1^{-1} - d)A^{p-1-k}B^{p-2}$ for $k = 0, \ldots, p-2$ and $\Omega_1^{-1}B^{p-2}$.
- 2^{nd} summation: Due to the condition $u + v \geq p$, the pair $(0, v)$ for $v = 0, \ldots, p-1$ cannot give the term $A^{p-1-k}B^{p-2}$. If $u = 1$, we then have $1 + v - p + 1 = p - 1 - k \Rightarrow v = 2p - 3 - k$. However, again, because of the condition $u+v \geq p$, we must have $v = p-1$. This can be possible only when $k = p - 2$. Hence, the second summation only contains the term dAB^{p-2}.
- 3^{rd} summation: We can ignore the case $u = 0$. If $u = 1$, then we have $1 + v - p = p - 1 - k$ and hence $v = 2p - k - 2$. Since $v \leq p - 1$, we have

$k \geq p-1 \Rightarrow k = p-1$ and hence $v = p-1$. This means that the third summation can only contain the term $d\overline{\Omega}B^{p-2}$.

Coefficient of $A^{p-1-k}B^{p-3}$ for $0 \leq k \leq p-3$.

Note that here u can be $0, 1$ or 2.

- 1^{st} summation: If $u = 0$, then we have $v = p-1-k$. This yields the coefficient $(-1)^k \Omega_1^{-2}$ for each k. Similarly, for each k, the coefficient is

$$\begin{cases} (-1)^k \left(-2d\Omega_1^{-1}\right) & \text{if } u = 1; \\ (-1)^k d^2 & \text{if } u = 2. \end{cases}$$

- 2^{nd} summation: If $u = 1$, then $1 + v - p + 1 = p - 1 - k \Rightarrow v = 2p - k - 3$. Since $u + v \geq p$, we must have $2p - k - 3 = p - 1 \Rightarrow k = p - 2$, which is not possible. Similarly, for $u = 2$, we have $(v, k) = (p-1, p-3)$ and this only gives the term $d^2 A^2 B^{p-3}$.

- 3^{rd} summation: Suppose that there exists (u, v) giving the term $A^{p-1-k}B^{p-3}$ for some k. Since $u + v - p = p - 1 - k$, we have $v = 2p - k - u - 1$. Because $v \leq p - 1$, we have $p - u \leq k$. However, due to the fact that $u \leq 2$, we have $p - 2 \leq k \leq p - 3$, a contradiction.

Writing all the terms from the above computation in descending colexicographical order and enclosing in square brackets those terms which will be absorbed in $\mathcal{E}$, we have:

$$\begin{aligned}\Lambda_1 A^{p-1}B^{p-1} =& - A^{p-2}B^{p-1} + \left[\sum_{k=0}^{p-3}(-1)^k A^{p-3-k}B^{p-1}\right] + \left(\Omega_1^{-1} - d\right) A^{p-1}B^{p-2} \\ &+ \left[\sum_{k=1}^{p-3}(-1)^k \left(\Omega_1^{-1} - d\right) A^{p-1-k}B^{p-2}\right] - \left[\left(\Omega_1^{-1} - 2d\right) AB^{p-2}\right] \\ &+ \left(d\overline{\Omega} + \Omega_1^{-1}\right) B^{p-2} + \left(\Omega_1^{-2} - 2d\Omega_1^{-1} + d^2\right) A^{p-1}B^{p-3} \\ &+ \left[\sum_{k=1}^{p-4}(-1)^k(\Omega_1^{-2} - 2d\Omega_1^{-1} + d^2)A^{p-1-k}B^{p-3}\right] \\ &+ \left[(\Omega_1^{-2} - 2d\Omega_1^{-1} + 2d^2)A^2B^{p-3}\right] + \mathcal{C}\left(A^2B^{p-3}\right). \qquad (*)\end{aligned}$$

Considering $(*)$, we see that we need $p > 3$ for the expression

$$\sum_{k=1}^{p-4}(-1)^k(\Omega_1^{-2} - 2d\Omega_1^{-1} + d^2)A^{p-1-k}B^{p-3}$$

to make sense.

Note that terms with colexicographical order lower than A^2B^{p-3} are absorbed in $\mathcal{C}\left(A^2B^{p-3}\right)$. This is because they all will be killed whatever their valuation is. It turns out later that the coefficients of the killers of these terms cannot affect us unlike those of the terms with colexicographical order higher than AB^{p-3}. This is the reason why we have to compute seriously in early steps.

Collecting terms enclosed in square brackets in $\mathcal{E}$, we have

$$\begin{aligned}\Lambda_1 A^{p-1}B^{p-1} =& - A^{p-2}B^{p-1} + \left(\Omega_1^{-1} - d\right) A^{p-1}B^{p-2} + \left(d\overline{\Omega} + \Omega_1^{-1}\right) B^{p-2} \\ &+ \left(\Omega_1^{-2} - 2d\Omega_1^{-1} + d^2\right) A^{p-1}B^{p-3} + \mathcal{E} + \mathcal{C}\left(A^2B^{p-3}\right).\end{aligned}$$

Hence, the first term we need to kill is

$$\left(\Omega_1^{-1} - d\right) A^{p-1}B^{p-2}$$

as it is the colexicographically highest term among terms not absorbed in $\mathcal{E}$.

Step 2: *Eliminate* $\left(\Omega_1^{-1} - d\right) A^{p-1}B^{p-2}$.

Due to Lemma 4.2.5, $\left(\Omega_1^{-1} - d\right) \Lambda_0$ is responsible for this task. By Proposition 4.1.2(i), we have

$$\begin{aligned}\left(\Omega_1^{-1} - d\right) \Lambda_0 A^{p-1}B^{p-1} = &- (\Omega_1^{-1} - d)A^{p-1}B^{p-2} \\ &+ (\Omega_1^{-1} - d)A^{p-1}B^{p-3} + \mathcal{C}\left(A^2B^{p-3}\right).\end{aligned}$$

Thus, we have

$$\begin{aligned}\left[\Lambda_1 + (\Omega_1^{-1} - d)\Lambda_0\right] A^{p-1}B^{p-1} = &-A^{p-2}B^{p-1} + \left(d\overline{\Omega} + \Omega_1^{-1}\right) B^{p-2} \\ &+ \left(\Omega_1^{-2} - (2d-1)\Omega_1^{-1} + d^2 - d\right) A^{p-1}B^{p-3} \\ &+ \mathcal{E} + \mathcal{C}\left(A^2B^{p-3}\right).\end{aligned}$$

Step 3: *Eliminate* $\left(d\overline{\Omega} + \Omega_1^{-1}\right) B^{p-2}$.

By Lemma 4.2.5, it is known that the colexicographically highest term in $\Lambda_0\Lambda_1^{p-1}A^{p-1}B^{p-1}$ is B^{p-2}. We then claim that the second colexicographically highest term in it is $-dA^2B^{p-3}$.

First, we consider

$$\Lambda_0\Lambda_1^{p-1}A^{p-1}B^{p-1} = \Lambda_1^{p-1}\left(-A^{p-1}B^{p-2} + A^{p-1}B^{p-3} + \mathcal{C}\left(A^2B^{p-3}\right)\right).$$

Since the colexicographically highest term in $\Lambda_1^{p-1}\left(A^{p-1}B^{p-3} + \mathcal{C}\left(A^2B^{p-3}\right)\right)$ is $-B^{p-3}$ which is colexicographically lower than A^2B^{p-3}, we can ignore it.

In terms of $\Lambda_1^{p-1}\left(-A^{p-1}B^{p-2}\right)$, Lemma 4.3.8 asserts that the coefficient of A^2B^{p-3} is precisely $-d$. Moreover, we show that A^rB^{p-3} does not appear in $\Lambda_1^{p-1}\left(-A^{p-1}B^{p-2}\right)$ when $r > 2$. We see that, from the mechanism of Λ_1 acting on A^rB^s explained in the proof of Proposition 4.2.7, only one Λ_1 can act by transferring degree from B to A (by exactly 1) otherwise the degree of B would have to be less than $p-3$. Hence, the $(p-2)$ Λ_1's must decrease degree of A and then

maximal degree of A is

$$(p-1)+1-(p-2)=2.$$

Hence, we have

$$\begin{aligned}-\left(d\overline{\Omega}+\Omega_1^{-1}\right)\Lambda_0\Lambda_1^{p-1}A^{p-1}B^{p-1} &= -\left(d\overline{\Omega}+\Omega_1^{-1}\right)B^{p-2}\\ &\quad+\left(d^2\overline{\Omega}+d\Omega_1^{-1}\right)A^2B^{p-3}+\mathcal{C}\left(A^2B^{p-3}\right).\end{aligned}$$

Thus, we have

$$\begin{aligned}&\left[\Lambda_1+(\Omega_1^{-1}-d)\Lambda_0-\left(d\overline{\Omega}+\Omega_1^{-1}\right)\Lambda_0\Lambda_1^{p-1}\right]A^{p-1}B^{p-1}\\ &\quad=-A^{p-2}B^{p-1}+\left(\Omega_1^{-2}-(2d-1)\Omega_1^{-1}+d^2-d\right)A^{p-1}B^{p-3}\\ &\qquad+(d^2\overline{\Omega}+\Omega_1^{-2}-d\Omega_1^{-1}+2d^2)A^2B^{p-3}+\mathcal{E}+\mathcal{C}\left(A^2B^{p-3}\right).\end{aligned}$$

Step 4: *Eliminate* $\left(\Omega_1^{-2}-(2d-1)\Omega_1^{-1}+d^2-d\right)A^{p-1}B^{p-3}$.

Since

$$\Lambda_0^2A^{p-1}B^{p-1}=2A^{p-1}B^{p-3}+\mathcal{C}(A^2B^{p-3}),$$

we use

$$-\frac{1}{2}\left(\Omega_1^{-2}-(2d-1)\Omega_1^{-1}+d^2-d\right)\Lambda_0^2$$

to kill $\left(\Omega_1^{-2}-(2d-1)\Omega_1^{-1}+d^2-d\right)A^{p-1}B^{p-3}$. Note that $-\frac{1}{2}$ is interpreted in $\mathbb{F}_p$ for $p\geq 5$ (or even for $p=3$) as $(p-3)!$ from the so-called Wilson's theorem.

For short, let us denote $(\Omega_1^{-1}-d)\Lambda_0-\left(d\overline{\Omega}+\Omega_1^{-1}\right)\Lambda_0\Lambda_1^{p-1}$ by Λ_2. Thus, we have

$$\begin{aligned}&\left[\Lambda_1+\Lambda_2-\frac{1}{2}\left(\Omega_1^{-2}-(2d-1)\Omega_1^{-1}+d^2-d\right)\Lambda_0^2\right]A^{p-1}B^{p-1}\\ &\quad=-A^{p-2}B^{p-1}+(d^2\overline{\Omega}+\Omega_1^{-2}-d\Omega_1^{-1}+2d^2)A^2B^{p-3}+\mathcal{E}+\mathcal{C}\left(A^2B^{p-3}\right).\end{aligned}$$

Step 5: *Eliminate* $(d^2\overline{\Omega}+\Omega_1^{-2}-d\Omega_1^{-1}+2d^2)A^2B^{p-3}$.

By Lemma 4.2.5, we have

$$(d^2\overline{\Omega} + \Omega_1^{-2} - d\Omega_1^{-1} + 2d^2)\Lambda_0^2\Lambda_1^{p-3}A^{p-1}B^{p-1} = -(d^2\overline{\Omega} + \Omega_1^{-2} - d\Omega_1^{-1} + 2d^2)A^2B^{p-3} + \mathcal{C}\left(A^2B^{p-3}\right).$$

Again, for short, let us denote $\Lambda_2 - \frac{1}{2}\left(\Omega_1^{-2} - (2d-1)\Omega_1^{-1} + d^2 - d\right)\Lambda_0^2$ by Λ_3. Hence, we have

$$\begin{aligned}&\left[\Lambda_1 + \Lambda_3 + (d^2\overline{\Omega} + \Omega_1^{-2} - d\Omega_1^{-1} + 2d^2)\Lambda_0^2\Lambda_1^{p-3}\right]A^{p-1}B^{p-1}\\ &\quad = -A^{p-2}B^{p-1} + \mathcal{E} + \mathcal{C}\left(A^2B^{p-3}\right).\end{aligned}$$

Step 6: *Eliminate every term absorbed in* $\mathcal{C}\left(A^2B^{p-3}\right)$.

As before, this step can be done by choosing appropriate elements in K together with using Lemma 4.2.5. Bear in mind that a systematic way to proceed is to eliminate terms in descending colexicographical order.

Every time we kill a term with colexicographical order lower than A^2B^{p-3}, we need to use $k_{i,j}\Lambda_0^i\Lambda_1^j$ for some $i, j \in \mathbb{S}_p$ and $k_{i,j} \in K$. Moreover, we have that the pair (i, j) must be *lexicographically higher* than $(2, p-3)$ (i.e. $i > 2$, or if $i = 2$ then $j > p-3$), which is denoted as $(i, j) \triangleright (2, p-3)$. This is because, omitting writing coefficients in K, we have that the colexicographically highest term in $\Lambda_0^i\Lambda_1^jA^{p-1}B^{p-1}$ is $A^{p-1-j}B^{p-1-i}$ by Lemma 4.2.5. Since $A^{p-1-j}B^{p-1-i} \prec A^2B^{p-3}$, we have $p-1-i < p-3$ or if $p-1-i = p-3$, then $p-1-j < 2$. This is equivalent to $i > 2$, or if $i = 2$ then $j > p-3$.

The ultimate outcome of the elimination process is that, for $p \geq 5$, we obtain

$$\begin{aligned}\Phi = {} & (\Omega_1^{-1} - d)\Lambda_0 - \left(d\overline{\Omega} + \Omega_1^{-1}\right)\Lambda_0\Lambda_1^{p-1}\\ & - \frac{1}{2}\left(\Omega_1^{-2} - (2d-1)\Omega_1^{-1} + d^2 - d\right)\Lambda_0^2\\ & + (d^2\overline{\Omega} + \Omega_1^{-2} - d\Omega_1^{-1} + 2d^2)\Lambda_0^2\Lambda_1^{p-3} + \sum_{(i,j)\triangleright(2,p-3)} k_{i,j}\Lambda_0^i\Lambda_1^j \qquad (5.1.1)\end{aligned}$$

for some $k_{i,j} \in K$. Especially, for $p \geq 5$, we have

$$v_L\left([\Lambda_1 + \Phi]\, A^{p-1}B^{p-1}\right) = v_L(A^{p-2}B^{p-1})$$

in every Hopf-Galois structure and for every choice of b and w.

Going back to the case $p = 3$, by using Maple, we show how to construct Φ step by step.

Step 1:

$$\begin{aligned}\Lambda_1 A^2B^2 = {} & 2AB^2 + B^2 + (\Omega_1^{-1} + 2d)A^2B + (2\Omega_1^{-1} + 2d)AB + (d\overline{\Omega} + \Omega_1^{-1})B \\ & + (d\Omega_1^{-1} + \Omega_1^{-2})A^2 + (\overline{\Omega} + d\Omega_1^{-1} + 2\Omega_1^{-2} + 1)A \\ & + 2\overline{\Omega} + 2d\Omega_1^{-1}\overline{\Omega} + \Omega_1^{-2} + 1.\end{aligned}$$

Step 2: To eliminate A^2B.

$$\begin{aligned}[\Lambda_1 + (\Omega_1^{-1} + 2d)\Lambda_0]A^2B^2 = {} & 2AB^2 + B^2 + (2\Omega_1^{-1} + 2d)AB + (d\overline{\Omega} + \Omega_1^{-1})B \\ & + \left((d+1)\Omega_1^{-1} + \Omega_1^{-2} + 2d\right)A^2 \\ & + \left(\overline{\Omega} + d\Omega_1^{-1} + 2\Omega_1^{-2} + 1\right)A \\ & + 2d\Omega_1^{-1}\overline{\Omega} + \Omega_1^{-2} + 1.\end{aligned}$$

Step 3: To eliminate B.

$$\begin{aligned}&[\Lambda_1 + (\Omega_1^{-1} + 2d)\Lambda_0 + (2d\overline{\Omega} + 2\Omega_1^{-1})\Lambda_0\Lambda_1^2]A^2B^2 \\ &\quad = 2AB^2 + B^2 + (2\Omega_1^{-1} + 2d)AB + (\overline{\Omega} + (2d+1)\Omega_1^{-1} + \Omega_1^{-2} + 2d)A^2 \\ &\qquad + (2d\Omega_1^{-1}\overline{\Omega} + \Omega_1^{-2} + 1)A + (d+1)\overline{\Omega} + 2d\Omega_1^{-1}\overline{\Omega} + (2d+1)\Omega_1^{-1} + \Omega_1^{-2} + 1.\end{aligned}$$

Step 4: To eliminate A^2.

$$\begin{aligned}[\Lambda_1 + (\Omega_1^{-1} + 2d)\Lambda_0 + (2d\overline{\Omega} + 2\Omega_1^{-1})\Lambda_0\Lambda_1^2 + (\overline{\Omega} + (2d+1)\Omega_1^{-1} + \Omega_1^{-2} + 2d)\Lambda_0^2]A^2B^2 \\ = 2AB^2 + B^2 + (2\Omega_1^{-1} + 2d)AB + \left(2d\Omega_1^{-1}\overline{\Omega} + \Omega_1^{-2} + 1\right)A \\ + (d+1)\overline{\Omega} + 2d\Omega_1^{-1}\overline{\Omega} + (2d+1)\Omega_1^{-1} + \Omega_1^{-2} + 1.\end{aligned}$$

Step 5: To eliminate A.

$$\begin{aligned}[\Lambda_1 + (\Omega_1^{-1} + 2d)\Lambda_0 + (2d\overline{\Omega} + 2\Omega_1^{-1})\Lambda_0\Lambda_1^2 + (\overline{\Omega} + (2d+1)\Omega_1^{-1} + \Omega_1^{-2} + 2d)\Lambda_0^2 \\ + (d\Omega_1^{-1}\overline{\Omega} + 2\Omega_1^{-2} + 2)\Lambda_0^2\Lambda_1]A^2B^2 \\ = 2AB^2 + B^2 + (2\Omega_1^{-1} + 2d)AB + (d+1)\overline{\Omega} + d\Omega_1^{-1}\overline{\Omega} + 2\Omega_1^{-2} + (2d+1)\Omega_1^{-1} + 2.\end{aligned}$$

Step 6: To eliminate 1_L.

$$\begin{aligned}[\Lambda_1 + (\Omega_1^{-1} + 2d)\Lambda_0 + (2d\overline{\Omega} + 2\Omega_1^{-1})\Lambda_0\Lambda_1^2 + (\overline{\Omega} + (2d+1)\Omega_1^{-1} + \Omega_1^{-2} + 2d)\Lambda_0^2 \\ + (d\Omega_1^{-1}\overline{\Omega} + 2\Omega_1^{-2} + 2)\Lambda_0^2\Lambda_1 \\ + 2\left((d+1)\overline{\Omega} + d\Omega_1^{-1}\overline{\Omega} + 2\Omega_1^{-2} + (2d+1)\Omega_1^{-1} + 2\right)\Lambda_0^2\Lambda_1^2]A^2B^2 \\ = 2AB^2 + B^2 + (2\Omega_1^{-1} + 2d)AB.\end{aligned}$$

Hence, we have

$$\begin{aligned}\Phi = (\Omega_1^{-1} + 2d)\Lambda_0 + (2d\overline{\Omega} + 2\Omega_1^{-1})\Lambda_0\Lambda_1^2 \\ + (\overline{\Omega} + (2d+1)\Omega_1^{-1} + \Omega_1^{-2} + 2d)\Lambda_0^2 + (d\Omega_1^{-1}\overline{\Omega} + 2\Omega_1^{-2} + 2)\Lambda_0^2\Lambda_1 \\ + 2\left((d+1)\overline{\Omega} + d\Omega_1^{-1}\overline{\Omega} + 2\Omega_1^{-2} + (2d+1)\Omega_1^{-1} + 2\right)\Lambda_0^2\Lambda_1^2\end{aligned}$$

and $[\Lambda_1 + \Phi]A^2B^2 = 2AB^2 + B^2 + (2\Omega_1^{-1} + 2d)AB$.

5.2 Proof of The Main Lemma

Proof of Lemma 5.1.3. (i) Done by the elimination process above. Note that, due to the construction, this result holds even in Hopf-Galois structures arising from

the special subgroup without putting any further assumption on b and w.

(ii) We first show the result when $p \geq 5$. Expressing $[\Lambda_1 + \Phi]B^{p-1}$ in terms of the basis A^iB^j with $0 \leq i, j \leq p-1$, we aim to show that the coefficient of A^{p-3} in $[\Lambda_1 + \Phi]B^{p-1}$ is $-2\overline{\Omega} - 2$. Note that this allows us to know an upper bound on $v_L\left([\Lambda_1 + \Phi]B^{p-1}\right)$. However, $-2\overline{\Omega}A^{p-3}$ is not necessarily the dominant term since we do not know coefficients of other basis elements.

Recall (5.1.1) for the definition of Φ. Since Λ_0 can only decrease degree of B, the killers

$$(\Omega_1^{-1} - d)\Lambda_0 \quad \text{and} \quad -\frac{1}{2}\left(\Omega_1^{-2} - (2d-1)\Omega_1^{-1} + d^2 - d\right)\Lambda_0^2$$

in Φ cannot give us A^{p-3}.

Then, we compute the coefficients of A^{p-3} from Λ_1 and the remaining killers in Φ acting on B^{p-1}.

From $\Lambda_1 B^{p-1}$.

Considering (4.1.1) in Proposition 4.1.2(ii), we see that $\Lambda_1 B^{p-1}$ gives A^{p-3} when $r = 0,\ t = 0,\ s = p-1$ and $u = p-3$. So, the coefficient of A^{p-3} is

$$(-1)^{p-3}(-d)^{p-3}\Omega_1^{-2} = d^{p-3}\Omega_1^{-2}.$$

From $-\left(d\overline{\Omega} + \Omega_1^{-1}\right)\Lambda_0\Lambda_1^{p-1}B^{p-1}$.

We first compute

$$\Lambda_0\Lambda_1^{p-1}B^{p-1} = \Lambda_1^{p-1}\left(-B^{p-2} + \mathcal{C}(B^{p-2})\right).$$

By Lemma 4.3.5(i), we have $d^{p-2}A^{p-3}$ is contained in $\Lambda_0\Lambda_1^{p-1}B^{p-1}$. Note that we can ignore $\mathcal{C}(B^{p-2})$ because of Proposition 4.2.7 and the fact that $\mathcal{C}(B^{p-2})$ contains only terms of type $B^k, k \leq p-3$. Therefore, we have that

$$-\left(d\overline{\Omega} + \Omega_1^{-1}\right)d^{p-2}A^{p-3} = \left(-\overline{\Omega} - d^{p-2}\Omega_1^{-1}\right)A^{p-3}$$

is contained in $-\left(d\overline{\Omega}+\Omega_1^{-1}\right)\Lambda_0\Lambda_1^{p-1}B^{p-1}$.

From $\left(d^2\overline{\Omega}+\Omega_1^{-2}-d\Omega_1^{-1}+2d^2\right)\Lambda_0^2\Lambda_1^{p-3}B^{p-1}$.

We compute

$$\Lambda_0^2\Lambda_1^{p-3}B^{p-1}=(p-1)(p-2)\Lambda_1^{p-3}\left(B^{p-3}+\mathcal{C}(B^{p-3})\right).$$

By Lemma 4.3.5(ii), we have

$$\left(d^2\overline{\Omega}+\Omega_1^{-2}-d\Omega_1^{-1}+2d^2\right)(p-1)(p-2)(p-3)!d^{p-3}=\left(-\overline{\Omega}-d^{p-3}\Omega_1^{-2}+d^{p-2}\Omega_1^{-1}-2\right)$$

is the coefficient of A^{p-3} from $\left(d^2\overline{\Omega}+\Omega_1^{-2}-d\Omega_1^{-1}+2d^2\right)\Lambda_0^2\Lambda_1^{p-3}B^{p-1}$. Note that we can ignore $\mathcal{C}(B^{p-3})$ since it contains only terms of type $B^k,\ k\leq p-4$ and even $\Lambda_1^{p-3}B^{p-4}$ cannot give A^{p-3} by Proposition 4.2.7.

Lastly, we show that $\sum_{(i,j)\triangleright(2,p-3)}k_{i,j}\Lambda_0^i\Lambda_1^jB^{p-1}$ fails to contain A^{p-3}. It is remarkable from Proposition 4.1.2(i) that the maximal degree of A in $\Lambda_0^i\Lambda_1^jB^{p-1}$ is equal to the maximal degree of A in $\Lambda_1^jB^{p-1-i}$.

If $j\leq p-1-i$, then, by Proposition 4.2.7, the maximal degree of A in $\Lambda_1^jB^{p-1-i}$ is at most

$$p-1-i<p-3$$

since (i,j) is lexicographically higher than $(2,p-3)$. If $j>p-1-i$, then the maximal degree of A is at most

$$\begin{aligned}2(p-1-i)-j&=2(p-1)-i-(i+j)\\&<2(p-1)-i-(p-1)=p-1-i\\&\leq p-3.\end{aligned}$$

As a result, we have that the coefficient of A^{p-3} in $[\Lambda_1+\Phi]\,B^{p-1}$ is

$$\left(d^{p-3}\Omega_1^{-2}\right)+\left(-\overline{\Omega}-d^{p-2}\Omega_1^{-1}\right)+\left(-\overline{\Omega}-d^{p-3}\Omega_1^{-2}+d^{p-2}\Omega_1^{-1}-2\right)=-2\overline{\Omega}-2$$

and the lemma follows for $p \geq 5$.

For $p = 3$, after doing a long calculation in Maple, we have

$$(\Lambda_1 + \Phi) B^2 = dAB + dB + A^2 + 2d\Omega_1^{-1} A + \overline{\Omega} + 1,$$

and hence $v_L ([\Lambda_1 + \Phi] B^2) \leq v_L \left(\overline{\Omega}\right)$. □

Remark. Λ_0 is responsible for decreasing degree of B. So we construct Φ to decrease degree of A in order that $-A^{p-2}B^{p-1}$ becomes the dominant term in $[\Lambda_1 + \Phi]A^{p-1}B^{p-1}$. If this was the case for the iteration of $\Lambda_1 + \Phi$, we would have a scaffold. Unfortunately, Lemma 5.1.3(ii) tells that this is impossible when B cannot completely dominate A. In particular, we see that some killers $k_{i,j}\Lambda_0^i\Lambda_1^j$ in Φ obstruct to have a scaffold by decreasing valuation sharply from certain coefficient $k_{i,j}$.

Chapter 6

Non-freeness of Ideals over Their Associated Orders

Thanks to the main Lemma, we can give the negative answer for the freeness of ideals over their associated orders in most Hopf-Galois structures on L/K. In the case of Hopf-Galois structures arising from non-special subgroups, the answer is unconditionally negative. However, in the case of the special subgroup, the main results vary on arithmetic conditions. The answer is still negative in most cases although there is a tiny gap which remains open. Moreover, under certain specific conditions, we show in the next chapter that scaffolds exist.

We begin this chapter by showing that, if, in some non-classical Hopf-Galois structure, there is an ideal which is free over its associated order, then

$$\mathbb{B} + 2p + 2 \geq 2\mathbb{A} \tag{6.0.1}$$

where $\mathbb{A} := -v_L(A)$ and $\mathbb{B} := -v_L(B)$. Moreover, this inequality can be used to show the non-freeness of ideals over their associated orders in most non-classical Hopf-Galois structures.

Assume that $\mathfrak{P}_L^h$ is free over its associated order $\mathfrak{A}$. For $i, j \in \mathbb{S}_{p^2}$, we put

$$c_{i,j} = \left\lceil \frac{h + i\mathbb{A} + j\mathbb{B}}{p^2} \right\rceil$$

where $\lceil x \rceil$ is the least integer that is greater than or equal to real number x. Then, $\{\pi_K^{c_{i,j}} A^i B^j : i, j \in \mathbb{S}_{p^2}\}$ is a generating set for $\mathfrak{P}_L^h$ over $\mathfrak{A}$.

Since, for $(i, j) \neq (p-1, p-1)$, we have

$$\Lambda_0^{p-1}\Lambda_1^{p-1} A^i B^j = 0 \;\text{ but }\; \Lambda_0^{p-1}\Lambda_1^{p-1} A^{p-1} B^{p-1} = 1,$$

we see that $\mathfrak{A}\pi_K^{c_{i,j}} A^i B^j \neq \mathfrak{P}_L^h$ due to Lemma 5.1.2. Since the ideal $\mathfrak{P}_L^h$ is free over $\mathfrak{A}$, then, by Theorem 5.1.1, $\pi_K^{c_{p-1,p-1}} A^{p-1} B^{p-1}$ is a generator. For brevity, let us write c instead of $c_{p-1,p-1}$.

With the notations $\mathbb{A}$ and $\mathbb{B}$, Lemma 5.1.3 can be restated as

$$v_L\left([\Lambda_1 + \Phi] A^{p-1} B^{p-1}\right) = -(p-2)\mathbb{A} - (p-1)\mathbb{B} \text{ and } v_L\left([\Lambda_1 + \Phi] B^{p-1}\right) \leq -(2p-3)\mathbb{A}.$$

After choosing

$$e = \left\lceil \frac{h + (p-2)\mathbb{A} + (p-1)\mathbb{B}}{p^2} \right\rceil - c$$

and

$$g = \left\lceil \frac{h + (p-1)\mathbb{B}}{p^2} \right\rceil,$$

we have $\pi_K^e(\Lambda_1 + \Phi) \in \mathfrak{A}$ because $\pi_K^e(\Lambda_1 + \Phi)\pi_K^c A^{p-1} B^{p-1} \in \mathfrak{P}_L^h$. Also, $\pi_K^g B^{p-1} \in \mathfrak{P}_L^h$. Hence, we have $\pi_K^e(\Lambda_1 + \Phi)\pi_K^g B^{p-1} \in \mathfrak{P}_L^h$, which implies that

$$v_L\left(\pi_K^e(\Lambda_1 + \Phi)\pi_K^g B^{p-1}\right) \geq h.$$

This yields the inequality

$$p^2(e+g) - (2p-3)\mathbb{A} \geq h \tag{6.0.2}$$

since $v_L\left([\Lambda_1+\Phi]B^{p-1}\right) \leq -(2p-3)\mathbb{A}$. Then, we have

$$p^2\left\lceil\frac{h+(p-2)\mathbb{A}+(p-1)\mathbb{B}}{p^2}\right\rceil - p^2\left\lceil\frac{h+(p-1)(\mathbb{A}+\mathbb{B})}{p^2}\right\rceil + p^2\left\lceil\frac{h+(p-1)\mathbb{B}}{p^2}\right\rceil - (2p-3)\mathbb{A} - h \geq 0. \tag{6.0.3}$$

In other words,

$$p^2\left\lceil\frac{h+(p-2)\mathbb{A}+(p-1)\mathbb{B}}{p^2}\right\rceil + p^2\left\lceil\frac{h+(p-1)\mathbb{B}}{p^2}\right\rceil \geq h + p^2\left\lceil\frac{h+(p-1)(\mathbb{A}+\mathbb{B})}{p^2}\right\rceil + (2p-3)\mathbb{A}.$$

Due to the fact that $m\left\lceil\frac{a}{m}\right\rceil \leq a+m-1$ for all $m \in \mathbb{N}$ and $a \in \mathbb{Z}$, it follows that

$$[h+(p-2)\mathbb{A}+(p-1)\mathbb{B}+p^2-1]+[h+(p-1)\mathbb{B}+p^2-1] \geq h+[h+(p-1)(\mathbb{A}+\mathbb{B})]+(2p-3)\mathbb{A}.$$

Collecting terms and dividing by $p-1$, this simplifies to

$$\mathbb{B}+2p+2 \geq 2\mathbb{A}.$$

Now, we are ready to show the non-freeness of ideals in non-classical Hopf-Galois structures.

6.1 Non-freeness in Hopf-Galois Structures Arising from Non-special Subgroups

Theorem 6.1.1. *In the Hopf-Galois structures arising from non-special subgroups, no ideal of $\mathfrak{O}_L$ is free over its associated order.*

Proof. Suppose for a contradiction that there exists an ideal $\mathfrak{P}_L^h$ which is free over its associated order $\mathfrak{A}$. Recall from Table 3 that in the non-special case,

$\mathbb{A} = p^2w + pb$ and $\mathbb{B} = b$. Then, by (6.0.1), we have

$$b \leq \frac{-2p^2w + 2p + 2}{2p - 1}.$$

Recall that $w \geq 0$. If $w > 0$, we have a contradiction as b is positive. This implies that the only possibility for $\mathfrak{P}_L^h$ to be free over the associated order is when $w = 0$ and $b = 1$

However, we can further show that the ideal cannot be free even when $w = 0$ and $b = 1$. Let us first record some necessary information:

(1) $v_L(\pi_K A^{p-1}B^{p-1}) = 1$,
(2) $v_L(\pi_K B^{p-1}) = p^2 - p + 1$,
(3) $v_L\left([\Lambda_1 + \Phi]\pi_K A^{p-1}B^{p-1}\right) = p + 1$,
(4) $v_L\left([\Lambda_1 + \Phi]\pi_K B^{p-1}\right) \leq 3p - p^2$.

Without loss of generality, let $h \in \{1, 2, ..., p^2\}$. Since the following arguments do not completely work when $p = 3$, let us assume that $p \geq 5$ at this moment.

If $h = 1$, we have $c = 1, e = 0$ and $g = 1$. Then, the equation (6.0.2) gives us a contradiction since

$$p^2 - (2p - 3)p = 3p - p^2 \not\geq h.$$

If $1 < h \leq p^2$, we have $c = 2$,

$$e = \begin{cases} -1 & \text{if } 1 < h \leq p + 1 \\ 0 & \text{if } h > p + 1, \end{cases}$$

and

$$g = \begin{cases} 1 & \text{if } h \leq p^2 - p + 1 \\ 2 & \text{if } h > p^2 - p + 1. \end{cases}$$

If $g = 1$, by (6.0.2), we have

$$h \leq p^2(e+1) - 2p^2 + 3p \leq -p^2 + 3p < 0.$$

If $g = 2$, we have

$$p^2 - p + 1 < h \leq p^2(e+2) - 2p^2 + 3p \leq 3p \Rightarrow p^2 + 1 < 4p.$$

Hence, for either value of g, we have a contradiction since $p \geq 5$.

For $p = 3$, we define a function as the LHS of (6.0.3):

$$\Delta(h) := 9\left\lceil \frac{h+5}{9} \right\rceil - 9\left\lceil \frac{h+8}{9} \right\rceil + 9\left\lceil \frac{h+2}{9} \right\rceil - 9 - h.$$

By using Maple, the values of Δ on $\{1, 2, \ldots, 9\}$ are shown in the table below.

h	1	2	3	4	5	6	7	8	9
$\Delta(h)$	-1	-11	-12	-13	-5	-6	-7	1	0

Table 4: Values of $\Delta(h)$

Due to (6.0.3), we obtain contradictions if $\Delta(h) < 0$. Hence, by Table 4, we have to deal with the cases when $h = 8$ and 9.

By trial and error, we find that $[\Lambda_1 + \Phi]\, AB^2$ can close the case. Recall that, for $p = 3$, we have

$$\begin{aligned}\Phi = {} & (\Omega_1^{-1} + 2d)\Lambda_0 + (2d\overline{\Omega} + 2\Omega_1^{-1})\Lambda_0\Lambda_1^2 \\ & + (\overline{\Omega} + (2d+1)\Omega_1^{-1} + \Omega_1^{-2} + 2d)\Lambda_0^2 + (d\Omega_1^{-1}\overline{\Omega} + 2\Omega_1^{-2} + 2)\Lambda_0^2\Lambda_1 \\ & + 2\left((d+1)\overline{\Omega} + d\Omega_1^{-1}\overline{\Omega} + 2\Omega_1^{-2} + (2d+1)\Omega_1^{-1} + 2\right)\Lambda_0^2\Lambda_1^2.\end{aligned}$$

By using Maple, letting $[\Lambda_1 + \Phi]$ act on AB^2, we have

$$[\Lambda_1 + \Phi]\, AB^2 = B^2 + dA^2B + 2dAB + \Omega_1^{-1}B + (2d\Omega_1^{-1} + 1)A^2 + (2\overline{\Omega} + 1)A + (2\overline{\Omega} + 1 + \Omega_1^{-1}d + 1).$$

We have:
(1) $v_L(A^2B^2) = -8$,
(2) $v_L(AB^2) = -5$,
(3) $v_L\left([\Lambda_1 + \Phi]\, A^2B^2\right) = -5$,
(4) $v_L\left([\Lambda_1 + \Phi]\, AB^2\right) = -12$.
Note that $\left(2\overline{\Omega} + 1\right) A$ is the dominant term in $[\Lambda_1 + \Phi]\, AB^2$ since $v_L(A) < 3v_L(B)$, $v_L\left(\overline{\Omega}\right) = 9$ and $v_L\left(\Omega_1\right) = 0$. Then, for $h = 8, 9$, we have $\pi_K^2 A^2B^2, \pi_K^2 AB^2 \in \mathfrak{P}_L^h$ and

$$v_L\left([\Lambda_1 + \Phi] \cdot \pi_K^2 A^2B^2\right) = 13 \geq h$$

but

$$v_L\left([\Lambda_1 + \Phi] \cdot \pi_K^2 AB^2\right) = 6 < h,$$

a contradiction. □

Remark. The main lemma (Lemma 5.1.3) can be applied to show the non-freeness of ideals over their associated orders provided that $v_L\left(\overline{\Omega}A^{p-3}\right)$ is highly negative. This is the case in Hopf-Galois structures arising from non-special subgroups since we have $v_L(A) \leq pv_L(B)$.

6.2 Non-freeness in Hopf-Galois Structures Arising from the Special Subgroup

The success in the proof of Theorem 6.1.1 is owing to the two facts. In Hopf-Galois structures arising from non-special subgroups, we have $v_L(A) \leq pv_L(B)$. Moreover, we can significantly increase degree of A so that the contradiction occurs by the influence of Φ. Unfortunately, in the case of the special subgroup, the

fact $v_L(A) \leq pv_L(B)$ does not always hold, so the main lemma is not sufficiently strong to cover this case. This is the reason why the result in this section diverges into several cases.

Throughout this section, we consider only Hopf-Galois structures arising from the special subgroup. We begin with providing a lemma giving a necessary condition for the non-freeness of ideals in the present situation. In this section, Ω is assumed to be non-unit (i.e. $w = -v_L(\Omega) > 0$) since otherwise it was exactly done in the previous theorem. Recall that $\mathbb{A} = -v_L(A) > 0$ and $\mathbb{B} = -v_L(B) > 0$.

Lemma 6.2.1. *In any Hopf-Galois structures arising from the special subgroup, if there exist $r, s \in \mathbb{N}$ such that*

$$r \geq s, \quad r\mathbb{A} > s\mathbb{B} \quad \textit{and} \quad \frac{s}{r} \geq \frac{1}{2} + \frac{1}{(p-1)w},$$

then no ideal of $\mathfrak{O}_L$ is free over its associated order.

Proof. Suppose that there exists an ideal $\mathfrak{P}_L^h$ which is free over its associated order $\mathfrak{A}$. Replacing $\mathbb{A}$ by pb and $\mathbb{B}$ by $p^2w + b$ in (6.0.1) gives us

$$(p^2w + b) + 2p + 2 \geq 2(pb)$$

and then

$$b \leq \frac{p^2w + 2p + 2}{2p - 1}. \tag{6.2.1}$$

The assumption $r\mathbb{A} > s\mathbb{B}$, equivalent to $b > \dfrac{p^2ws}{pr-s}$, yields

$$\begin{aligned}
\frac{p^2ws}{pr-s} < \frac{p^2w+2p+2}{2p-1} &\Leftrightarrow (2p-1)p^2ws < (pr-s)\left(p^2w+2p+2\right)\\
&\Leftrightarrow (2p-1)p^2ws < (pr-s)p^2w + (pr-s)(2p+2)\\
&\Leftrightarrow (2s-r)p^3w < 2(pr-s)(p+1)\\
&\Leftrightarrow (2s-r)p^2w < 2(p+1)\left(r-\frac{s}{p}\right)\\
&\Rightarrow (2s-r)\left(p^2-1\right)w < 2(p+1)r\\
&\Leftrightarrow \frac{s}{r} < \frac{1}{2} + \frac{1}{(p-1)w}, \quad \text{a contradiction.}
\end{aligned}$$

□

Due to Lemma 6.2.1, the roles of b and w can affect the non-freeness of ideals over their associated orders. To close the study, we classify all the possibilities of b and w in terms of $\mathbb{A}$ and $\mathbb{B}$ into 4 cases as below:

1. $\dfrac{\mathbb{A}}{\mathbb{B}} < \dfrac{1}{2}$,
2. $\dfrac{1}{2} < \dfrac{\mathbb{A}}{\mathbb{B}} < \dfrac{2}{3}$,
3. $\dfrac{2}{3} < \dfrac{\mathbb{A}}{\mathbb{B}} < 1$, and
4. $1 < \dfrac{\mathbb{A}}{\mathbb{B}}$.

Note that in the four cases, the equality can be dropped since $p \geq 3$ and $\mathbb{A}$ is not congruent to $\mathbb{B}$ modulo p.

It is remarkable that case 1 and 2 cannot be addressed by Lemma 6.2.1. In fact, it is found that scaffolds exists in case 1 (see the next chapter). A special treatment is required for case 2. Yet, there is an unsolved remaining gap in this case. For case 3 and 4, we have:

Theorem 6.2.2. *No ideal of $\mathfrak{O}_L$ is free over its associated order in Hopf-Galois structures arising from the special subgroup provided that $\dfrac{2}{3} < \dfrac{\mathbb{A}}{\mathbb{B}} < 1$ or $1 < \dfrac{\mathbb{A}}{\mathbb{B}}$.*

Proof. By Lemma 6.2.1, it is obvious when $1 < \frac{\mathbb{A}}{\mathbb{B}}$. We see that the last condition, $\frac{2}{3} < \frac{\mathbb{A}}{\mathbb{B}} < 1$, satisfies Lemma 6.2.1 except when $p = 3,\ w = 1, 2$ or $p = 5,\ w = 1$.

For each p, knowing w, we can compute for b via the inequality

$$\frac{2}{3} < \frac{\mathbb{A}}{\mathbb{B}} < 1 \ \Leftrightarrow\ \frac{2p^2w}{3p-2} < b < \frac{p^2w}{p-1}.$$

Recall that $p \nmid b$. Therefore, we have to deal with

$$(p, b, w) = (3, 4, 1), (3, 7, 2), (3, 8, 2), (5, 4, 1), (5, 6, 1).$$

According to the LHS of (6.0.3), we define

$$\begin{aligned}\Delta_p(h, b, w) \ :=\ & p^2\left\lceil \frac{h + (p-2)pb + (p-1)(p^2w + b)}{p^2} \right\rceil \\ & - p^2\left\lceil \frac{h + (p-1)\left(p^2w + (p+1)b\right)}{p^2} \right\rceil \\ & + p^2\left\lceil \frac{h + (p-1)(p^2w + b)}{p^2} \right\rceil - (2p-3)pb - h \\ =\ & p^2\left\lceil \frac{h - b(p+1)}{p^2} \right\rceil - p^2\left\lceil \frac{h-b}{p^2} \right\rceil + p^2\left\lceil \frac{h + b(p-1)}{p^2} \right\rceil \\ & + p^2w(p-1) - (2p-3)pb - h. \end{aligned} \tag{6.2.2}$$

Then, we compute values of $\Delta_p(h, b, w)$ by using Maple as shown in Table 5 and Table 6.

h	1	2	3	4	5	6	7	8	9
$\Delta_3(h, 4, 1)$	-19	-11	-12	-13	-23	-24	-25	-17	-18
$\Delta_3(h, 7, 2)$	-37	-29	-30	-31	-23	-24	-25	-35	-36
$\Delta_3(h, 8, 2)$	-46	-47	-39	-40	-41	-33	-34	-35	-45

Table 5: Values of $\Delta_3(h, b, w)$

h	$\Delta_5(h,4,1)$	$\Delta_5(h,6,1)$	h	$\Delta_5(h,4,1)$	$\Delta_5(h,6,1)$
1	-16	-111	14	-29	-99
2	-17	-87	15	-30	-100
3	-18	-88	16	-31	-101
4	-19	-89	17	-32	-102
5	-45	-90	18	-33	-103
6	-46	-91	19	-34	-104
7	-47	-117	20	-35	-105
8	-48	-118	21	-36	-106
9	-49	-119	22	-37	-107
10	-25	-120	23	-38	-108
11	-26	-121	24	-39	-109
12	-27	-97	25	-15	-110
13	-28	-98			

Table 6: Values of $\Delta_5(h,b,w)$

Since every value in both tables is negative, we are done. □

Now, it is time for the most complicated case $\frac{1}{2} < \frac{\mathbb{A}}{\mathbb{B}} < \frac{2}{3}$. Equivalently,

$$\frac{p^2w}{2p-1} < b < \frac{2p^2w}{3p-2}.$$

In the light of the main lemma (Lemma 5.1.3), (6.2.1) says that if

$$b > \frac{p^2w}{2p-1} + \left(1 + \frac{3}{2p-1}\right)$$

then no ideal of $\mathfrak{O}_L$ can be free over its associated order. Thus, for each w, the unknown range in terms of b is shrunk as

$$\left(\frac{p^2w}{2p-1}, \frac{p^2w}{2p-1} + \left(1 + \frac{3}{2p-1}\right)\right).$$

Hence, the range can contain at most two choices for b as far as only the main lemma is concerned.

One of the goals of this thesis is to minimize those choices for b to be at most only one. Moreover, in the unknown case, we also provide a necessary but not sufficient condition to determine which ideal $\mathfrak{P}_L^h$ of $\mathfrak{O}_L$ cannot be free over its associated order. Sadly, as the condition is not sufficient, there are some ideals

with which our technique cannot cope.

Fix $w \in \mathbb{N}$ and an ideal $\mathfrak{P}_L^h$. In order to address the unknown range in terms of b, we set

- $b = \dfrac{p^2 w}{2p-1} + \varepsilon$ for some $0 < \varepsilon < 1 + \dfrac{3}{2p-1}$ so that $b \in \mathbb{N}$ and $p \nmid b$.
- $\mathcal{A} := \Delta_p(h, b, w)$. See (6.2.2).
- $\mathcal{B} := p^3 w - p^2 w + 2p^2 - b\,(2p^2 - 3p + 1)\,.$
- $\mathcal{D} := \left\lceil \dfrac{h - b(p+1)}{p^2} \right\rceil - \left\lceil \dfrac{h-b}{p^2} \right\rceil + \left\lceil \dfrac{h + b(p-1)}{p^2} \right\rceil.$
- $\dfrac{h-b}{p^2} = s + \dfrac{t}{p^2}$ and $\dfrac{bp}{p^2} = x + \dfrac{y}{p^2}$ for some $s, t, x, y \in \mathbb{Z}$ where $0 \leq t < p^2$ and $y \in \{p, 2p, \ldots, (p-1)p\}\,.$

It can be first observed that

$$\mathcal{B} - \mathcal{A} = 2p^2 + h - b - p^2\mathcal{D}.$$

Bear in mind that, due to (6.0.3), we want $\mathcal{A}$ to be negative to obtain a contradiction. The only difficulty in the calculation is how to deal with ceiling functions in $\mathcal{D}$. Analysing the cases of the parameters t and y, we can break those ceiling functions and compute the term $\mathcal{B} - \mathcal{A}$ as shown in the table below.

Case	$\left\lceil \frac{h-b(p+1)}{p^2} \right\rceil$	$\left\lceil \frac{h-b}{p^2} \right\rceil$	$\left\lceil \frac{h+b(p-1)}{p^2} \right\rceil$	$\mathcal{D}$	$\mathcal{B}-\mathcal{A}$
$y<t, t+y>p^2$	$s-x+1$	$s+1$	$s+x+2$	$s+2$	t
$y<t, t+y\leq p^2$	$s-x+1$	$s+1$	$s+x+1$	$s+1$	p^2+t
$y\geq t>0, t+y>p^2$	$s-x$	$s+1$	$s+x+2$	$s+1$	p^2+t
$y\geq t>0, t+y\leq p^2$	$s-x$	$s+1$	$s+x+1$	s	$2p^2+t$
$y>t=0$	$s-x$	s	$s+x+1$	$s+1$	p^2+t

Table 7: Computing $\mathcal{D}$ and $\mathcal{B}-\mathcal{A}$

According to the table, we can say in general that

$$\mathcal{A}=\mathcal{B}-ap^2-t$$

for some $a\in\{0,1,2\}$. Substituting $b=\dfrac{p^2w}{2p-1}+\varepsilon$, we have

$$\mathcal{A}=(2-a)p^2-\varepsilon(2p^2-3p+1)-t.$$

Then, the theorem below summarises a necessary condition for $\mathfrak{P}_L^h$ to be not free over its associated order.

Theorem 6.2.3. *Assume that* $\dfrac{1}{2}<\dfrac{\mathbb{A}}{\mathbb{B}}<\dfrac{2}{3}$. *With the notations defined above, the ideal* $\mathfrak{P}_L^h$ *is not free over its associated order in* $L\left[N_{\langle\nu\rangle,d}\right]^G$ *if the parameters* t, y *and* ε *fall into any of the following cases:*

(i) $y<t, t+y>p^2$ *and* $t>2p^2-\varepsilon(2p^2-3p+1)$,

(ii) $y<t, t+y\leq p^2$ *and* $t>p^2-\varepsilon(2p^2-3p+1)$,

(iii) $y\geq t>0, t+y>p^2$ *and* $t>p^2-\varepsilon(2p^2-3p+1)$,

(iv) $y \geq t > 0$ *and* $t + y \leq p^2$,

(v) $y > t = 0$ *and* $\varepsilon > \dfrac{p^2}{2p^2 - 3p + 1}$.

Proof. This is straightforward from considering Table 7 and the inequality

$$\mathcal{A} = (2 - a)p^2 - \varepsilon(2p^2 - 3p + 1) - t < 0.$$

□

Remark. Although t and y must fall into any case in Table 7, it is possible that relations of p, t and ε do not meet any condition in Theorem 6.2.3. In this case, we have $\mathcal{A}$ is nonnegative. In other words, we cannot say whether the ideal $\mathfrak{P}_L^h$ is free or not.

With the full potential of the technique in this thesis, the following theorem is drawn on the condition that all the ideals must behave uniformly.

Theorem 6.2.4. *Assume that* $\dfrac{1}{2} < \dfrac{\mathbb{A}}{\mathbb{B}} < \dfrac{2}{3}$. *If* $\varepsilon > \dfrac{3p+2}{4p-2}$, *then no ideal is free over its associated order in Hopf-Galois structures arising from the special subgroup.*

Proof. The idea is to find a unified condition satisfying all the cases in Theorem 6.2.3 in terms of ε. Hence, case (iv) can be ignored. Considering case (i), we compute the possible least value of t satisfying $y < t,\ t + y > p^2$. Since $y \in \{p, 2p, \ldots, (p-1)p\}$, we have

$$t + \frac{p(p-1)}{2} > p^2, \text{ which is equivalent to } t > \frac{p^2 + p}{2}, \text{ and hence } t \geq \frac{p^2 + p + 2}{2}.$$

Thus, to satisfy case (i) for all possible t's, we must have

$$\frac{p^2 + p + 2}{2} > 2p^2 - \varepsilon(2p^2 - 3p + 1) \Leftrightarrow \varepsilon > \frac{3p^2 - p - 2}{4p^2 - 6p + 2} = \frac{3p+2}{4p-2}.$$

Moreover, since this condition can fulfil every condition in every remaining case (except case (iv)), we are done. □

Corollary 6.2.5. *A necessary condition for the non-freeness of all the ideals of the valuation ring over their associated orders for $p \geq 3$ is $\varepsilon > 1.1$. In particular, the condition can be relaxed to $\varepsilon > \frac{17}{18}$ if $p \geq 5$.*

Proof. This is an immediate result of Theorem 6.2.4. □

Remark. If $\varepsilon \leq \frac{3p+2}{4p-2}$, it means that there are some ideals for which we cannot determine the freeness status. However, ideals satisfying any case in Theorem 6.2.3 can be determined as 'not free'. To see a picture of all the unknown cases, it is worth mentioning the least choice for b. From the assumption $\frac{1}{2} < \frac{\mathbb{A}}{\mathbb{B}} < \frac{2}{3}$, they are

$$\begin{cases} 1 + \dfrac{p^2 w}{2p-1} & \text{if } \ 2p-1 \mid w, \\ \left\lceil \dfrac{p^2 w}{2p-1} \right\rceil & \text{if } \ 2p-1 \nmid w \text{ and } p \nmid \left\lceil \dfrac{p^2 w}{2p-1} \right\rceil, \\ 1 + \left\lceil \dfrac{p^2 w}{2p-1} \right\rceil & \text{if } \ 2p-1 \nmid w \text{ but } p \mid \left\lceil \dfrac{p^2 w}{2p-1} \right\rceil. \end{cases}$$

By Theorem 6.2.4, for $p \geq 5$, the only case when some ideals could be free is when

$$2p-1 \nmid w, \ p \nmid \left\lceil \frac{p^2 w}{2p-1} \right\rceil, \ b = \left\lceil \frac{p^2 w}{2p-1} \right\rceil \text{ and } b - \frac{p^2 w}{2p-1} \leq \frac{3p+2}{4p-2}.$$

For $p = 3$, the unknown cases are

$$b = \begin{cases} \dfrac{9w}{5} + 1 & \text{if } \ 5 \mid w, \\ \left\lceil \dfrac{9w}{5} \right\rceil & \text{if } \ 5 \nmid w \text{ and } 3 \nmid \left\lceil \dfrac{9w}{5} \right\rceil. \end{cases}$$

Note that although the necessary condition for non-freeness of every ideal in Corollary 6.2.5 is $\varepsilon > 1.1$, we can exclude the case

$$b = \left\lceil \frac{9w}{5} \right\rceil + 1 \ \text{ if } \ 5 \nmid w \text{ but } 3 \mid \left\lceil \frac{9w}{5} \right\rceil$$

from the list of the least choices for b. This is because

$$b - \frac{9w}{5} = \left(\left\lceil \frac{9w}{5} \right\rceil - \frac{9w}{5} \right) + 1 \geq \frac{1}{5} + 1 = 1.2 > 1.1.$$

In conclusion, when b is sufficiently greater than $\dfrac{p^2 w}{2p-1}$, there are not any ideals of the valuation ring free over their associated orders in Hopf-Galois structures arising from the special subgroup.

Chapter 7

Scaffolds

Previously, in Hopf-Galois structures arising from the special subgroup, we classified the relation of $\mathbb{A}$ and $\mathbb{B}$ into 4 cases. This chapter is responsible for investigating the remaining case $\frac{\mathbb{A}}{\mathbb{B}} < \frac{1}{2}$. Since, in this case, the valuation of B can sufficiently dominate A, we can construct scaffolds of precision ∞.

7.1 Description of Scaffolds

Although, in this chapter, we write expressions with parameters in unified language, we interpret them only in Hopf-Galois structures arising from the special subgroup. Hence, in this chapter, we have $v_L(A) = -pb,\ v_L(B) = -p^2w - b$ and $v_L(\Omega_1) = p^2w$. Also, due to the condition $\frac{\mathbb{A}}{\mathbb{B}} < \frac{1}{2}$, we have $v_L(B) < 2v_L(A)$. Of course, the difference cannot be seen in the algebraic viewpoint. Yet, there is a huge impact once arithmetic properties come into play.

Due to Proposition 4.1.2(i), it is obvious to see that the dominant term (the term determining the valuation) in $\Lambda_0^i A^r B^s$ for $i \leq s$ is

$$s(s-1)\cdots(s-i+1)A^rB^{s-i}.$$

Then, to have a scaffold, we have to find an element in $L\left[N_{\langle\nu\rangle,d}\right]^G$, say Γ_1, with

the property that for $j \leq r$

$$v_L\left(\Gamma_1^j A^r B^s\right) = v_L\left(A^{r-j} B^s\right).$$

Then, we show that $\Lambda_1 + \Upsilon$ where

$$\Upsilon := \sum_{t=1}^{p-1} (p-t-1)! \Omega_1^{-t} \Lambda_0^t$$

has such a desired property thanks to the condition $\dfrac{\mathbb{A}}{\mathbb{B}} < \dfrac{1}{2}$. Indeed, Υ is a product of the elimination process in Chapter 5 but the extra condition $\dfrac{\mathbb{A}}{\mathbb{B}} < \dfrac{1}{2}$ is added when we compare the valuation to decide which terms need to be eliminated. Recall that, in Chapter 5, we use only the fact given in Definition 5.1.4. Before seeing that $\Lambda_1 + \Upsilon$ satisfies the property, we need the lemma below.

Lemma 7.1.1. *Suppose that* $\dfrac{\mathbb{A}}{\mathbb{B}} < \dfrac{1}{2}$. *Let* $1 \leq s \leq p-1$ *and* $0 \leq r \leq p-1$. *Then, the dominant term in*

$$\sum_{(u,t) \neq (0,0)} \binom{s}{u} \binom{r}{t} (-d)^u A^{r-t+u} \left(B - \Omega_1^{-1}\right)^{s-u},$$

where $u \leq s, t \leq r$, *is* $\begin{cases} rA^{r-1}B^s & \text{if } r \geq 1 \\ -dsAB^{s-1} & \text{if } r = 0. \end{cases}$

Proof. In this computation, we can omit writing elements from $\mathbb{F}_p$ since their valuation is 0. Also note that since $v_L(B) = -p^2 w - b < -p^2 w = v_L(\Omega_1^{-1})$, we can consider only the term $A^{r-t+u} B^{s-u}$ in

$$A^{r-t+u}(B - \Omega_1^{-1})^{s-u}.$$

In other words, it suffices to find the dominant term in

$$\sum_{(u,t) \neq (0,0)} \binom{s}{u} \binom{r}{t} (-d)^u A^{r-t+u} B^{s-u}.$$

Let $r \geq 1$. Suppose that there exist $f \in \{0, 1, \ldots, s\}$ and $g \in \{0, 1, \ldots, r\}$ with $(f, g) \neq (0, 0)$ such that $v_L(A^{r-g+f}B^{s-f}) < v_L(A^{r-1}B^s)$. Then, we have

$$v_L(A^{f-g+1}) < v_L(B^f).$$

If $f = 0$, we must have $1 - g > 0$ implying that $g = 0$. This is not possible because $(f, g) \neq (0, 0)$. Now, we assume that $f \geq 1$. Then, we consider

$$v_L(A^{f+1}) \leq v_L(A^{f-g+1}) < v_L(B^f).$$

This gives us

$$\frac{\mathbb{A}}{\mathbb{B}} > \frac{f}{f+1} \geq \frac{1}{2},$$

a contradiction.

If $r = 0$, we see that

$$\sum_{(u,t)\neq(0,0)} \binom{s}{u}\binom{r}{t}(-d)^u A^{r-t+u}B^{s-u} = \sum_{u=1}^{s}(-d)^u \binom{s}{u} A^u B^{s-u},$$

which has valuation $v_L\left(AB^{s-1}\right)$ since $v_L(B) < v_L(A)$. □

The lemma below asserts that $\Lambda_1 + \Upsilon$ satisfies the desired property to have a scaffold.

Lemma 7.1.2. *Suppose that* $\dfrac{\mathbb{A}}{\mathbb{B}} < \dfrac{1}{2}$. *Let* $1 \leq r \leq p-1$ *and* $0 \leq s \leq p-1$. *We have*

(i) $v_L\left(\left(\Lambda_1 + \Upsilon\right) A^r B^s\right) = v_L\left(A^{r-1}B^s\right)$.

(ii) $v_L\left(\left(\Lambda_1 + \Upsilon\right)\alpha\right) \geq v_L(\alpha) + \mathbb{A}$ *for all* $\alpha \in L$.

(iii) $v_L\left(\left(\Lambda_1 + \Upsilon\right)^i A^r B^s\right) = v_L\left(A^{r-i}B^s\right)$ *for* $r \geq i \geq 1$.

Proof. (i) We first compute

$$\begin{aligned}\Upsilon A^r B^s &= \sum_{t=1}^{p-1}(p-t-1)!\Omega_1^{-t}\Lambda_0^t A^r B^s \\ &= A^r \sum_{t=1}^{p-1}(p-t-1)!\Omega_1^{-t}\Lambda_0^t B^s \\ &= A^r\left[\sum_{t=1}^{s}(p-t-1)!\Omega_1^{-t}\left(t!\binom{s}{t}B^{s-t}+\sum_{z\geq 1}f_z\delta_{s,t+z}B^{s-t-z}\right)\right]\end{aligned}$$

for some $f_z \in \mathbb{F}_p$ and where $\delta_{i,j} = \begin{cases} 1 & \text{if } i \geq j, \\ 0 & \text{otherwise.} \end{cases}$

By Wilson's theorem, it can be shown that

$$(p-t-1)!t! \equiv (-1)^{t+1} \pmod{p}.$$

This gives us

$$\begin{aligned}\Upsilon A^r B^s = &-\sum_{t=1}^{s}(-1)^t\binom{s}{t}\Omega_1^{-t}A^r B^{s-t} \\ &+\sum_{t=1}^{s}\sum_{z\geq 1}(p-t-1)!f_z\delta_{s,t+z}\Omega_1^{-t}A^r B^{s-t-z}.\end{aligned}$$

Then, recall the formula (4.1.1)

$$\Lambda_1 A^r B^s = \sum_{u=0}^{s}\sum_{t=0}^{r}\binom{s}{u}\binom{r}{t}(-d)^u A^{r-t+u}(B-\Omega_1^{-1})^{s-u} + \sum_{v=0}^{r}\binom{r}{v}\delta_{s,p-1}A^v - A^r B^s$$

or equivalently, expanding the term $u = t = 0$ in the first sum,

$$\begin{aligned}\Lambda_1 A^r B^s = &\sum_{\ell=1}^{s}(-1)^\ell\binom{s}{\ell}\Omega_1^{-\ell}A^r B^{s-\ell} + \sum_{v=0}^{r}\binom{r}{v}\delta_{s,p-1}A^v \\ &+\sum_{(u,t)\neq(0,0)}\binom{s}{u}\binom{r}{t}(-d)^u A^{r-t+u}(B-\Omega_1^{-1})^{s-u}.\end{aligned}$$

It follows that

$$(\Lambda_1 + \Upsilon)\, A^r B^s = \sum_{t=1}^{s} \sum_{z\geq 1} (p-t-1)! f_z \delta_{s,t+z} \Omega_1^{-t} A^r B^{s-t-z} + \sum_{v=0}^{r} \binom{r}{v} \delta_{s,p-1} A^v + \sum_{(u,t)\neq(0,0)} \binom{s}{u}\binom{r}{t} (-d)^u A^{r-t+u} (B - \Omega_1^{-1})^{s-u}. \tag{7.1.1}$$

It is obvious that

$$v_L\left(\sum_{t=1}^{s} \sum_{z\geq 1} (p-t-1)! f_z \delta_{s,t+z} \Omega_1^{-t} A^r B^{s-t-z}\right) \geq \begin{cases} v_L(\Omega_1^{-1} A^r B^{s-2}) & \text{if } s \geq 2 \\ \infty & \text{otherwise.} \end{cases}$$

and

$$v_L\left(\sum_{v=0}^{r} \binom{r}{v} \delta_{s,p-1} A^v\right) = \begin{cases} v_L\left(A^r\right) & \text{if } s = p-1 \\ \infty & \text{otherwise.} \end{cases}$$

Next, by Lemma 7.1.1, we have

$$v_L\left(\sum_{(u,t)\neq(0,0)} \binom{s}{u}\binom{r}{t} (-d)^u A^{r-t+u} (B - \Omega_1^{-1})^{s-u}\right) = v_L\left(rA^{r-1}B^s\right)$$

To find the dominant term in (7.1.1), we first see that

$$v_L\left(rA^{r-1}B^s\right) < v_L\left(\sum_{v=0}^{r} \binom{r}{v} \delta_{s,p-1} A^v\right)$$

for all $0 \leq s \leq p-1$. In fact, we see that $v_L\left(rA^{r-1}B^s\right) < v_L\left(A^r\right)$ if $s \geq 1$ due to the assumption $\dfrac{\mathbb{A}}{\mathbb{B}} < \dfrac{1}{2}$. The assumption also implies that $v_L(B) < v_L(A)$ and hence $v_L\left(B^2\right) < v_L\left(\Omega_1^{-1} A\right)$. The latter inequality is equivalent to

$$v_L\left(rA^{r-1}B^s\right) < v_L\left(\Omega_1^{-1} A^r B^{s-2}\right)$$

for $s \geq 2$. This proves (i).

(ii) Without loss of generality, we may assume that $\alpha = kA^xB^y$ for some $x, y \in \mathbb{S}_p$ and $k \in K$. If $x \geq 1$, by (i), we have

$$v_L\left((\Lambda_1 + \Upsilon)\,\alpha\right) = v_L((\Lambda_1 + \Upsilon)\,kA^xB^y) = v_L(kA^{x-1}B^y) = v_L(\alpha) + \mathbb{A}.$$

Now assume that $x = 0$. It also suffices to assume that $y \geq 1$. Considering the derivation of (7.1.1), we have that

$$\begin{aligned}(\Lambda_1 + \Upsilon)\,B^y = &\sum_{t=1}^{y}\sum_{z\geq 1}(p-t-1)!f_z\delta_{y,t+z}\Omega_1^{-t}B^{y-t-z} \\ &+ \sum_{u=1}^{y}\binom{y}{u}(-d)^uA^u(B-\Omega_1^{-1})^{y-u}.\end{aligned}$$

To find the dominant term in $(\Lambda_1 + \Upsilon)\,B^y$, we see that

$$v_L\left(\sum_{t=1}^{y}\sum_{z\geq 1}(p-t-1)!f_z\delta_{y,t+z}\Omega_1^{-t}B^{y-t-z}\right) \geq \begin{cases} v_L(\Omega_1^{-1}B^{y-2}) & \text{if } y \geq 2 \\ \infty & \text{otherwise;}\end{cases}$$

and

$$v_L\left(\sum_{u=1}^{y}\binom{y}{u}(-d)^uA^u(B-\Omega_1^{-1})^{y-u}\right) = v_L\left(-dyAB^{y-1}\right)$$

since $v_L(B) < v_L(A)$ and $v_L(B) < v_L\left(\Omega_1^{-1}\right)$. Then, it is easy to see that

$$v_L\left((\Lambda_1 + \Upsilon)\,B^y\right) = v_L\left(-dyAB^{y-1}\right)$$

since $v_L\left(B\right) < v_L\left(\Omega_1^{-1}\right)$. Thus, we have

$$v_L\left((\Lambda_1 + \Upsilon)\,kB^y\right) = v_L(kB^y) + \mathbb{B} - \mathbb{A} > v_L(kB^y) + \mathbb{A}$$

since $\dfrac{\mathbb{A}}{\mathbb{B}} < \dfrac{1}{2}$. This proves (ii).

(iii) This follows immediately from (i) and (ii). Note that (ii) guarantees that the iteration can be done. □

Finally, we are ready to introduce the scaffolds constructed in this thesis. For short, let us put $\Gamma_0 := \Lambda_0$ and $\Gamma_1 := \Lambda_1 + \Upsilon$. The theorem below asserts that Γ_0 and Γ_1 are ingredients of the scaffolds.

Theorem 7.1.3. *The field extension L/K possesses an $L[N_{\langle\nu\rangle,d}]^G$-scaffold of precision ∞ with the shift parameters $b_1 := b < b + p^2w =: b_2$ provided that $\dfrac{\mathbb{A}}{\mathbb{B}} < \dfrac{1}{2}$, which is equivalent to $b_2/b_1 > 2p$.*

In particular, the scaffold constructed in this thesis consists of:

- *shift parameters $b_1 = b$ and $b_2 = b + p^2w$,*
- *the collection $\{\lambda_t \in L : t \in \mathbb{Z}\}$ with $\lambda_t = \pi_K^f \Gamma_1^{s_0} \Gamma_0^{s_1} A^{p-1} B^{p-1}$ where $s = s_1 p + s_0 \in \mathbb{S}_{p^2}$ and $f \in \mathbb{Z}$ is chosen such that $p^2 f + v_L(A^{p-1}B^{p-1}) + \mathfrak{b}(s) = t$ (the construction of λ_t is guided by some part of the proof of Theorem A.1(ii) in [BCE] and the existence of f is due to the fact that $\{\mathfrak{b}(s) : s \in \mathbb{S}_{p^2}\}$ is a complete set of residues modulo p^2),*
- *the collection of $\{\Gamma_0, \Gamma_1\}$.*

Proof. Let $s \in \mathbb{S}_{p^2}$. Then, $s = s_1 p + s_0$ for some $s_0, s_1 \in \mathbb{S}_p$. By Proposition 4.1.2(i) and Lemma 7.1.2(iii) we have

$$\begin{aligned} v_L\left(\Gamma_0^{s_0}\Gamma_1^{s_1}A^{p-1}B^{p-1}\right) &= v_L(A^{p-1-s_1}B^{p-1-s_0}) \\ &= v_L(A^{p-1}B^{p-1}) + s_1 p b_1 + s_0 b_2 \\ &= v_L(A^{p-1}B^{p-1}) + \mathfrak{b}(s). \end{aligned}$$

Since $\Lambda_0 \cdot 1 = \Lambda_1 \cdot 1 = 0$ and $\Lambda_0^p = \Lambda_1^p = 0$, we have

$$\Gamma_0 \cdot 1 = \Gamma_1 \cdot 1 = 0 \quad \text{and} \quad \Gamma_0^p = \Gamma_1^p = 0.$$

Then, the theorem follows from Theorem 2.4.5. □

Chapter 8

Consequences and Conclusion

The consequences in this chapter are immediately derived through Theorem 2.4.8, the main theorem of [BCE], with the assistance of the main theorems in this thesis. Eventually, in the last section, we provide the final theorem summarising all the core materials in this study.

Recall that $\{b_1 := b, b_2 := b + p^2w\}$ is the set of ramification break numbers for L/K. Thus, we have $\mathbb{A} = pb_1$ and $\mathbb{B} = b_2$ in Hopf-Galois structures arising from the special subgroup. Then, we state theorems in this final chapter through the concept of the ramification break numbers.

8.1 Freeness Condition

As scaffolds of precision ∞ exist in Hopf-Galois structures arising from the special subgroup, we can employ them to determine which ideals of the valuation ring can be free over their associated orders. Recall (2.4.3) and (2.4.4) for the definitions of $\mathfrak{d}$ and $\mathfrak{w}$, respectively.

Theorem 8.1.1. *In Hopf-Galois structures arising from the special subgroup together with the condition $b_2/b_1 > 2p$, an ideal $\mathfrak{P}_L^h$ is free over its associated iff $\mathfrak{w}(s) = \mathfrak{d}(s)$ for all $s \in \mathbb{S}_{p^2}$.*

Proof. This immediately follows from Theorem 2.4.8(ii). Note that the map $\mathfrak{d}$ in our context is defined as

$$\mathfrak{d}(s) = \left\lfloor \frac{s_1 pb + s_0(b + p^2 w) + \mathscr{B} - h}{p^2} \right\rfloor$$

where $s = s_1 p + s_0$ and $\mathscr{B} \in \mathbb{S}_{p^2}(h)$ such that $\mathfrak{a}\left(\mathfrak{r}(\mathscr{B})\right) = p^2 - 1$. □

Under the assumption in Theorem 8.1.1, we provide the necessary and sufficient condition for $\mathfrak{O}_L$ (i.e. $\mathfrak{P}_L^h$ with $h = 0$) to be free over its associated order $\mathfrak{A}$ in the example below. However, since it is not easy to check the condition $\mathfrak{w}(s) = \mathfrak{d}(s)$ for all $s \in \mathbb{S}_{p^2}$, we state an equivalent form of the condition but much simpler to digest.

Example 8.1.2. In $L\left[N_{\langle\nu\rangle,d}\right]^G$, if $b_2/b_1 > 2p$, then $\mathfrak{O}_L$ is free over $\mathfrak{A}$ iff $\mathfrak{r}(b)$ divides $p^2 - 1$. This is due to [BCE, Theorem 4.8].

8.2 Non-existence of Scaffolds

The negative answer to the question of the freeness of ideals is obtained in most Hopf-Galois structures. This gives rise to the non-existence of scaffolds due to the theorem below.

Theorem 8.2.1. *Let L/K be a totally ramified extension of degree p^n. In a Hopf-Galois structure H, if a scaffold exists, then there is an ideal free over its associated order.*

Proof. Choose $\mathscr{B} \in \mathbb{S}_{p^n}$ such that $\mathfrak{a}(\mathscr{B}) = p^n - 1$. Then, we claim that $\mathfrak{P}_L^{\mathscr{B}}$ is free over its associated order due to the fact that $\mathfrak{w}(s) = \mathfrak{d}(s)$ for all $s \in \mathbb{S}_{p^n}$ with $h = \mathscr{B}$ as in Theorem 2.4.8(i).

Assume that $s = \sum_{i=1}^{n} s_{(n-i)} p^{n-i}$ and $j = \sum_{i=1}^{n} j_{(n-i)} p^{n-i}$. By putting $h = \mathscr{B}$, we simply have

$$\mathfrak{d}(s) = \left\lfloor \frac{\mathfrak{b}(s)}{p^n} \right\rfloor$$

and $$\mathfrak{w}(s) = \min\left\{ \left\lfloor \frac{\mathfrak{b}(s+j)}{p^n} \right\rfloor - \left\lfloor \frac{\mathfrak{b}(j)}{p^n} \right\rfloor : j \in \mathbb{S}_{p^n},\ j \preceq p^n - 1 - s \right\}.$$

Since $j \underset{n}{\preceq} p^n - 1 - s$, we have $s_{(n-i)} + j_{(n-i)} \leq p-1$ for $1 \leq i \leq n$. Then, $s + j = \sum_{i=1}^{n} \left(s_{(n-i)} + j_{(n-i)}\right) p^{n-i}$ and hence $\mathfrak{b}(s+j) = \mathfrak{b}(s) + \mathfrak{b}(j)$.

By the definition, $\mathfrak{w}(s) \leq \mathfrak{d}(s)$. On the other hand, we have

$$\mathfrak{d}(s) = \left\lfloor \frac{\mathfrak{b}(s)}{p^n} \right\rfloor \leq \left\lfloor \frac{\mathfrak{b}(s) + \mathfrak{b}(j)}{p^n} \right\rfloor - \left\lfloor \frac{\mathfrak{b}(j)}{p^n} \right\rfloor$$

for all j such that $j \preceq p^n - 1 - s$. Note that the inequality above follows from the fact $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$. This gives us $\mathfrak{d}(s) \leq \mathfrak{w}(s)$. □

8.3 Conclusion

Theorem 8.3.1. *Let L/K be a near one-dimensional elementary abelian extension of degree p^2 and $L[N_{T,d}]^G$ a Hopf-Galois structure we consider.*
(I) No ideal is free over its associated order and hence scaffolds do not exist provided that

(i) L/K has only one ramification break number;

(ii) L/K has two ramification break numbers and T is a non-special subgroup or

(iii) L/K has two ramification break numbers, T is the special subgroup and
$b_2/b_1 < p$
$p < b_2/b_1 < 3p/2$ *or*
$3p/2 < b_2/b_1 < 2p$ *and* $2pb_1 - b_2 > 1.1(2p-1)$.

(II) In Hopf-Galois structures arising from the special subgroup, if $2p < b_2/b_1$, then a scaffold exists with the description conveyed in Theorem 7.1.3. Moreover, the necessary and sufficient condition for an ideal to be free over its associated order is that $\mathfrak{w}(s) = \mathfrak{d}(s)$ for all $s \in \mathbb{S}_{p^2}$.

Bibliography

[BCE] Nigel P. Byott, Lindsay N. Childs, and G. Griffith Elder, *Scaffolds and Generalized Integral Galois Module Structure*, Annales de l'institut Fourier **68** (2018), no. 3, 965-1010.

[BE14] Nigel P. Byott and G. Griffith Elder, *Integral Galois Module Structure for Elementary Abelian Extensions with a Galois Scaffold*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3705–3712.

[BE18] Nigel P. Byott and G. Griffith Elder, *Sufficient conditions for large Galois scaffolds*, J. Number Theory **182** (2018), 95-130.

[By02] Nigel P. Byott, *Integral Hopf-Galois Structures on Degree p^2 Extensions of p-adic Fields*, J. Algebra **248** (2002), 334–365.

[By96] Nigel P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), 3217–3228, Corrigendum, ibid., 3705.

[By97] Nigel P. Byott, *Galois Structure of Ideals in Wildly Ramified Abelian p-extension of a p-adic Field, and Some Applications*, Journal de theorie des nombres de Bordeaux **9** (1997), no. 2, 449-462.

[Ch00] Lindsay N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, Mathematical Surveys and Monographs **80**, Amer. Math. Soc., Providence, RI, 2000.

[Ef06] Ido Efrat, *Valuations, Orderings, and Milnor K-theory* , Mathematical Surveys and Monographs **124**, Amer. Math. Soc., Providence, 2006.

[El09] G. Griffith Elder, *Galois Scaffolding in One-dimensional Elementary Abelian Extensions*, Proc. Amer. Math. Soc. **137** (2009), no. 4, 1193–1203.

[EP05] Antonio J. Engler and Alexander Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005.

[Fr83] Albrecht Fröhlich, *Galois Module Structure of Algebraic Integers*, Springer, 1983.

[FV93] Ivan B. Fesenko and Sergei V. Vostokov, *Local Fields and Their Extensions: A Constructive Approach*, Translations of Mathematical Monographs **121**, American Mathematical Society, Providence, RI, 1993.

[Ko14] Alan Koch, *Hopf Galois structures on primitive purely inseparable extensions*, New York J. Math. **20** (2014), 779–797.

[Se79] Jean-Pierre Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[Tr09] Paul J. Truman, *Hopf-Galois Module Structure of Some Tamely Ramified Extensions*, Ph.D. thesis, University of Exeter, 2009.

[Un11] Robert G. Underwood, *An Introduction to Hopf Algebras*, Springer, New York Dordrecht Heidelberg London, 2011.

[Un15] Robert G. Underwood, *Fundamentals of Hopf Algebras*, Springer, Cham Heidelberg New York Dordrecht London, 2015.